



Federal Register

**Monday,
December 30, 2002**

Part III

**Department of
Transportation**

Coast Guard

Maritime Security; Notice

DEPARTMENT OF TRANSPORTATION**Coast Guard****[USCG-2002-14069]****Maritime Security****AGENCY:** Coast Guard, DOT.**ACTION:** Notice of meetings; request for comments.

SUMMARY: The Coast Guard is holding seven public meetings to discuss requirements for security assessments, plans, and specific security measures for ports, vessels, and facilities. Discussions will aid the Coast Guard in determining the types of vessels and facilities that pose a risk of being involved in a transportation security incident, and in identifying security measures and standards to deter such incidents. Discussions will also focus on aligning domestic maritime security requirements with the International Ship and Port Facility Security (ISPS) Code and recent amendments to the International Convention for the Safety of Life at Sea (SOLAS), to comply with section 102 (Port security) of the recently enacted Maritime Transportation Security Act of 2002 (MTSA). We encourage interested individuals and organizations to attend the meetings and submit comments for discussion during the meetings. We also seek comments from anyone unable to attend the meetings.

DATES: The public meetings will be held on the following dates and at the following locations.

- January 27, 2003, 9 a.m. to 5 p.m., New Orleans, LA.
- January 30, 2003, 2 p.m. to 7 p.m., Cleveland, OH.
- January 31, 2003, 12 (noon) to 6 p.m., St. Louis, MO.
- February 3, 2003, 9 a.m. to 5 p.m., Seattle, WA.
- February 5, 2003, 9 a.m. to 5 p.m., Los Angeles-Long Beach, CA.
- February 7, 2003, 9 a.m. to 5 p.m., Jacksonville, FL.
- February 11, 2003, 9 a.m. to 5 p.m., New York City, NY.

Comments and related material intended for inclusion in the public docket (USCG-2002-14069) must reach the Docket Management Facility on or before February 28, 2003. Comments and related material containing protected information, such as proprietary or security information, intended for inclusion in the Coast Guard's internal docket for protected information also must reach the Coast Guard's Office of Regulations and Administrative Law (G-LRA) on or before February 28, 2003.

ADDRESSES: The meetings will be held at the following locations:

- New Orleans, LA—Hilton Riverside, 2 Poydras St., New Orleans, LA 70140.
- Cleveland, OH—Sheraton Cleveland City Centre Hotel, Dorothy Fuldheim Room, 777 St. Clair Ave., Cleveland, OH 44144.
- St. Louis, MO—Robert A. Young Federal Building (R.A.Y. Building), 1222 Spruce St., St. Louis, MO 63017.
- Seattle, WA—Boeing Field, 7755 East Marginal Way South, Building 2-22, Auditorium, Seattle, WA 98108.
- Los Angeles-Long Beach, CA—Port of Los Angeles, 425 S. Palos Verdes St., San Pedro, CA 90731.
- Jacksonville, FL—Florida Department of Law Enforcement (FDLE), 921 N. Davis St., Building E, Jacksonville, FL 32209.
- New York City, NY—Customs House Auditorium, Alexander Hamilton U.S. Customs House, 1 Bowling Green, New York, NY 10004.

You may submit your public comments directly to the Docket Management Facility. Please see the *Request for Comments* section below for more information regarding submitting comments that contain protected information. To make sure that your public comments and related material do not enter the docket (USCG-2002-14069) more than once, please submit them by only one of the following means:

- (1) Electronically through the Web Site for the Docket Management System at <http://dms.dot.gov/>.
- (2) By fax to the Docket Management Facility at 202-493-2251.
- (3) By delivery to room PL-401 on the Plaza level of the Nassif Building, 400 Seventh Street, SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202-366-9329.
- (4) By mail to the Docket Management Facility, (USCG-2002-14069), U.S. Department of Transportation, room PL-401, 400 Seventh Street, SW., Washington, DC 20590-0001.

The Docket Management Facility maintains the public docket for this notice. Comments and material received from the public, as well as documents mentioned in this notice as being available in the public docket, will become part of this public docket and will be available for inspection or copying at room PL-401 on the Plaza level of the Nassif Building, 400 Seventh Street, SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. You may also find this notice in the

public docket on the Internet at <http://dms.dot.gov/>.

Anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review the Department of Transportation's complete Privacy Act Statement in the **Federal Register** published on April 11, 2000 (65 FR 19477-78), or you may visit <http://dms.dot.gov/>.

Comments containing protected information, as explained in the *Request for Comments* section below, must be submitted in writing and must be mailed or hand-delivered to Commandant (G-LRA)/Room 3406, U.S. Coast Guard Headquarters, 2100 Second Street, SW., Washington, DC 20593.

FOR FURTHER INFORMATION CONTACT: For information concerning this notice or the public meetings, write or call Mr. Martin Jackson of the Office of Standards Evaluation and Development (G-MSR), U.S. Coast Guard Headquarters, 2100 Second Street, SW., Washington, DC 20593, mjackson@comdt.uscg.mil, or at 202-267-1140.

For questions regarding submissions of protected information, contact Ms. Kathryn Sinniger of the Office of Regulations and Administrative Law (G-LRA), U.S. Coast Guard Headquarters, 2100 Second Street, SW., Washington, DC 20593, or at 202-267-1534.

For questions on viewing or submitting material to the public docket, call Ms. Dorothy Beard, Chief of Dockets, Department of Transportation, at 202-366-5149.

SUPPLEMENTARY INFORMATION:**Request for Comments**

We encourage you to participate in these meetings by submitting comments and related material. If you do so, please include your name and address, identify the docket number (USCG-2002-14069) and give the reason for each comment.

If you wish to submit any protected information in your comments, you must submit your comment by mail or hand delivery to the Office of Regulations and Administrative Law (G-LRA) at the address under

ADDRESSES. Protected information includes confidential or privileged business or commercial information that is not normally released to the public. It also includes security information that, if released, would be detrimental to the safety of persons in transportation.

Examples of the latter include vulnerability assessments (or portions thereof), specific security actions to be taken by your company or vessel, and draft plans that would comply with the International Ship and Port Facility Security (ISPS) Code or any of the Navigation and Vessel Inspection Circulars (NVICs) referenced in this notice. Please be sure to indicate whether the entire submission constitutes protected information, or if it is only portions of the submission that need to be protected. If the latter, please identify those portions which constitute protected information clearly within your submission. If you are submitting confidential or privileged business information, please explain, within your submission, how this information is normally treated within your company or organization.

You may submit your public comments and material electronically, by fax, by delivery, or by mail to the Docket Management Facility at the address under **ADDRESSES**; but please submit your public comments and material by only one means. If you submit them by mail or delivery, submit them in an unbound format, no larger than 8½ by 11 inches, suitable for copying and electronic filing. If you submit them by mail and would like to know that they reached the Facility, please enclose a stamped, self-addressed postcard or envelope. We will consider all comments and material received during the comment period.

Public Meetings

The Coast Guard encourages the following individuals and organization representatives to attend the public meetings:

- Owners and operators of vessels, facilities, and other structures located on or adjacent to U.S. navigable waters;
- Federal, State, and local agencies in law enforcement and emergency planning;
- Port authorities;
- State and local government organizations;
- Shipping agents;
- Insurance companies;
- Protection and Indemnity Clubs;
- Classification societies;
- Maritime industry associations; and
- Other interested persons.

Meeting attendees will have the opportunity to orally comment on topics scheduled for discussion on the agenda. Appendix A provides the intended format of the meetings. We may ask questions to clarify comments given by an attendee. Unless otherwise noted, the meetings will be held each day from 9 a.m. to 5 p.m. on the dates and locations

identified under **DATES** and **ADDRESSES**. Attendees will be responsible for making their own arrangements for lunch at the mid-day break, scheduled for 1 p.m. each day. The meetings will reconvene at 2 p.m. and are scheduled to end at 5 p.m. We may end the meetings early if we have covered all of the agenda topics and if the people attending have no further comments. All statements, questions and answers, or comments made orally at the public meetings will become part of the public docket. In addition to these public meetings, the Coast Guard will request its Federal Advisory Committees, as appropriate, to include maritime security issues and the content of this notice on their agendas in order to provide further opportunities for comment.

Information on Services for Individuals With Disabilities

To obtain information on facilities or services for individuals with disabilities or to ask that we provide special assistance at the meetings, please notify Mr. Martin Jackson at the address or phone number under **FOR FURTHER INFORMATION CONTACT**.

Background and Purpose

In the aftermath of September 11, 2001, the Commandant of the Coast Guard reaffirmed the Coast Guard's Maritime Homeland Security mission and its lead role, in coordination with the Department of Defense; Federal, State, and local agencies; owners and operators of vessels and maritime facilities; and others with interests in our nation's marine transportation system, to detect, deter, disrupt, and respond to attacks against U.S. territory, population, vessels, facilities, and critical maritime infrastructure by terrorist organizations.

In November 2001, the Commandant of the Coast Guard addressed the International Maritime Organization (IMO) General Assembly, urging that body to consider an international scheme for port and shipping security. Recommendations and proposals for comprehensive security requirements, including amendments to SOLAS and the new ISPS Code, were developed at a series of intersessional maritime security work group meetings held at the direction of the IMO's Maritime Safety Committee.

The Coast Guard submitted comprehensive security proposals to the intersessional maritime security work group meetings based on work it had been coordinating since October 2001. Prior to each intersessional meeting, the Coast Guard held public meetings as

well as coordinated several industry meetings with representatives from major U.S. and foreign associations for shipping, labor, and ports. Maritime security was also a major agenda item at Federal Advisory Committee meetings held by the Coast Guard during the past year. Additional meetings were also held with Federal agencies having complementary security responsibilities.

In January 2002, the Coast Guard held a two-day public workshop in Washington, DC, attended by more than 300 individuals, including members of the public and private sectors, and representatives of the national and international marine industry (66 FR 65020, December 17, 2001; docket number USCG-2001-11138). Their comments indicated the need for specific threat identification, analysis of threats, and methods for developing performance standards to plan for response to maritime threats.

Additionally, the public comments stressed the importance of uniformity in the application and enforcement of requirements and the need to establish threat levels with a means to communicate threats to the marine transportation system.

The Coast Guard considered and advanced U.S. proposals for maritime security that took into account this public and agency input. We consider the International Convention for the Safety of Life at Sea (SOLAS) amendments and the ISPS Code, as adopted by the International Maritime Organization (IMO) Diplomatic Conference in December 2002, to reflect current industry, public, and agency concerns. The entry into force date of both the ISPS Code and related SOLAS amendments is July 1, 2004, with the exception of the Automatic Identification System (AIS) whose implementation was accelerated to no later than December 31, 2004, depending on the particular class of SOLAS vessel.

Domestically, the Coast Guard had previously developed regulations for security that are contained in 33 CFR parts 120 and 128. Complementary guidance can be found in Navigation and Vessel Inspection Circular (NVIC) 3-96, Change 2, Security for Passenger Vessels and Passenger Terminals. Prior to development of additional regulations, the Coast Guard, with input from the public, needed to assess the current state of port and vessel security and their vulnerabilities. As mentioned previously, to accomplish this, the Coast Guard conducted a public workshop January 28-30, 2002, to assess existing Maritime Transportation System

security standards and measures and to gather ideas on possible improvements. Based on the comments received at the workshop, the Coast Guard cancelled NVIC 3-96 (Security for Passenger Vessels and Passenger Terminals) and issued a new NVIC 4-02 (Security for Passenger Vessels and Passenger Terminals) that incorporated guidelines consistent with international initiatives (the ISPS Code and SOLAS amendments). Additional NVICs were also published, including NVIC 9-02 (Guidelines for Port Security Committees, and Port Security Plans Required for U.S. Ports), NVIC 10-02 (Security Guidelines for Vessels); and NVIC 11-02 (Security Guidelines for Facilities [not yet available]). The documents are or will be available in the public docket (USCG-2002-14069) for review at the locations under

ADDRESSES.

On November 25, 2002, President George W. Bush signed into effect Public Law 107-295, the Maritime Transportation Security Act of 2002 (MTSA), which had been proposed to Congress the year before as the Port and Maritime Security Act (S. 1214). The MTSA requires the Secretary to issue an interim final rule, as soon as practicable, as a temporary regulation to implement the Port Security section of the Act. The MTSA expressly waives the requirements of the Administrative Procedure Act, including notice and comment, for this purpose. Nevertheless, the Coast Guard believes it is important to get the preliminary views of the public, especially affected maritime interests, prior to issuing the interim final rule. The temporary interim rule may be superseded by a final rule within one year of the enactment of the MTSA. The requirements of MTSA section 102 directly align with the security requirements embodied in the SOLAS amendments and ISPS Code; however, the MTSA has broader application that includes domestic vessels and facilities. Thus, the Coast Guard intends to implement the MTSA through the requirements in the SOLAS amendments and the ISPS Code parts A and B for all vessels and facilities that are currently required to meet SOLAS, as well as those vessels exclusively on domestic trade and facilities that are at risk of being involved in a transportation security incident.

The Coast Guard considers that the implementation of these requirements is best done through mandating compliance with the SOLAS amendments and the ISPS Code including part A and part B (see Appendix B). The Coast Guard

considers part B an essential element to ensure full and effective compliance with the intent of the MTSA. Foreign flag vessels entering the U.S. would be expected to verify compliance with part B or provide proof that any alternatives are equivalent to that part. Verification of compliance could be established by flag administration documents or endorsements that indicate that the Ship Security Certificate was issued based upon full compliance with part B.

Because of the broad application in the MTSA, the discussions in this notice use the term "vessels" rather than the term "ships" as found in the SOLAS amendments and the ISPS Code. These terms can be used interchangeably but serve to emphasize the Coast Guard's intention to apply security measures to those vessels we have determined are at risk of being involved in a transportation security incident.

In addition, under MTSA, the terms "Area Maritime Transportation Security Plan" means a Port Security Plan developed in accordance with NVIC 9-02; "Area Security Advisory Committee" means the Port Security Committee; and "Federal Maritime Security Coordinator" means the cognizant Captain of the Port. The Coast Guard intends to align any future rulemaking with the MTSA terminology.

The Coast Guard plans to publish a temporary interim rule no later than June 2003 and a final rule by November 2003. These dates are critical in order to uniformly implement the ISPS Code and SOLAS amendments, as well as meet the urgency set by the mandates in the MTSA.

As such, the Coast Guard is announcing seven public meetings and requesting comments that will aid them in drafting the mandated interim rule and final rule.

What Will Be Discussed at the Public Meetings?

Attendees should be prepared to discuss the implementation of SOLAS amendments and ISPS Code, including application to vessels engaged in domestic voyages in accordance with the MTSA, as well as domestic implications of implementing the recommended security measures described in recently published guidance (NVICs).

How Should I Prepare for the Public Meeting?

Attendees should review the SOLAS amendments and ISPS Code, published NVICs, existing regulations in 33 CFR parts 120 and 128, section 102 of the MTSA, preliminary cost analysis, and

associated supporting documents to evaluate the feasibility of recommended or required security measures.

The ISPS Code and SOLAS amendments, and the preliminary costs analysis are included in this notice as Appendix B and Appendix C, respectively. The NVICs, MTSA, related public comments, and associated supporting documents are available for review in the public docket (USCG-2002-14069) at the locations under

ADDRESSES.

After evaluating these documents, the public should then prepare statements to be presented at the meetings or submit to the public docket (USCG-2002-14069) expressing any concerns and suggesting ways to implement the required measures. Attendees also should propose possible equivalencies to the SOLAS amendments and ISPS Code, and the MTSA requirements.

Who Should Attend the Public Meetings?

Port Stakeholders. While the Coast Guard will be primarily responsible for ensuring the new SOLAS amendments and ISPS Code, and section 102 of the MTSA for U.S. ports are implemented through the development of Port Security Plans and establishment of Port Security Committees, we will need the cooperation of other Federal agencies, port authorities, State and local governments, local emergency responders, maritime industry associations, facility and vessel owners and operators and other port community stakeholders such as the owners of other structures located on or adjacent to U.S. navigable waters.

Because Port Security Plans are overarching and address many areas of the maritime community, the plans will apply to commercial vessels and facilities, as well as to such entities as—

- Recreational vessels and uninspected passenger vessels.
- Nautical school vessels and sailing school vessels.
- Small passenger vessels on domestic voyages.
- Uninspected fishing vessels.
- Oil spill response vessels.
- Military installations and vessels.
- Facilities that transfer, store, or otherwise handle dry bulk or general cargo.
- Marinas.
- Ship repair facilities.
- Waterfront areas that are densely populated or host large public events.
- Other areas within the port that are critical to port operations or public safety.

Vessel Owners, Operators, and Charterers. Requirements are being

considered for operators of certain vessels to develop Vessel Security Assessments and Plans, designate Company and Vessel Security Officers, and implement security measures (see Appendix A). The Coast Guard considers these security measures to be integral for vessel security and appropriate for the majority of vessels operating in U.S. waters. Therefore, the Coast Guard would apply these requirements to such commercial vessels as—

- All foreign ships, both cargo and passenger, required to comply with SOLAS;
- All foreign ships, both cargo and passenger, of countries not signatory to SOLAS;
- All vessels subject to 46 CFR subchapter I (cargo vessels);
- All vessels subject to 46 CFR subchapter L (offshore supply vessels);
- All passenger vessels subject to 46 CFR subchapters H and K;
- All passenger vessels subject to 46 CFR subchapter T engaged on an International voyage;
- All barges subject to 46 CFR subchapters D, I, and O;
- All tankships subject to 46 CFR subchapters D and O;
- All Mobile Offshore Drilling Units (MODUs) subject to 46 CFR subchapter I–A; and
- All towing vessels greater than 6 meters in registered length.

Facility Owners or Operators.

Requirements are being considered for operators of certain facilities to develop Facility Security Assessments and Plans, designate Facility Security Officers, and implement security measures (see Appendix A). The Coast Guard considers these security measures to be integral for facility security and appropriate for the majority of facilities servicing vessels that operate in U.S. waters or facilities that are on or adjacent to U.S. waters and pose a risk to them. Therefore, the Coast Guard would apply these requirements to such facilities as—

- Facilities that handle cargo regulated under 33 CFR parts 126, 127, and 154;
- Facilities that service vessels certified to carry more than 150 passengers; and
- Facilities that receive vessels on international voyages including vessels solely navigating the Great Lakes.

As an Affected Entity, What Information Should I Bring to the Public Meetings?

Attendees should bring their recommendations and responses to the questions provided in Appendix A. Attendees should also be prepared to

offer their best practices with regard to the security issues and comments on application, implementation and operating costs.

What Will Be the Format of the Public Meetings?

The public meetings will follow a question-answer format. A facilitator will describe the SOLAS amendment and ISPS Code requirements and the Coast Guard's implementation strategy. The facilitator then will pose a series of questions and solicit attendees' responses. We will discuss, in this order, general security provisions, port security provisions, vessel security provisions, facility security provisions, and other security provisions. Appendix A provides the intended format of the meetings.

What Other Information Would Assist the Coast Guard in Drafting the Temporary Interim Security Rule?

We request information about all current Federal, State, and local governmental laws, procedures, regulations, and standards that are either functioning or that are planned. We also request industry to provide any current and planned standards and procedures covering the security of vessels and facilities, and recommendations toward additional regulations.

What Are the Estimated Costs of Implementing the SOLAS Amendments, the ISPS Code, and Section 102 of the MTSA, as Discussed in This Notice?

For the purposes of good business practice and in order to comply with regulations promulgated by other Federal and State agencies, many companies have spent, to date, a substantial amount of money and resources to upgrade and improve security. The costs discussed in Appendix C do not include resources these companies have already spent to enhance security. To estimate costs, we contacted operators to determine what specific security improvements they had made and the costs they had incurred since the events of September 11, 2001. We found that these operators were reluctant to share their information with us. Consequently, the estimates in the following analysis are based heavily on Coast Guard judgments.

We realize that each company engaged in maritime commerce would not implement the ISPS Code exactly as presented in this analysis. Depending on each company's choices, some companies could spend much less than what is estimated herein while others could spend significantly more. In

general, we assume that each company would implement the ISPS Code based on the types of vessels and facilities it owns or operates and whether it engages in international or domestic trade.

Based on this analysis, the first year cost would be approximately \$1.4 billion, with costs of approximately Present Value (PV) \$6.0 billion over the next 10 years (2003–2012, 7 percent discount rate). The preliminary cost analysis in Appendix C presents the costs in three sections: vessel security, facility security, and port security. The following is a summary of the preliminary cost analysis.

- *Vessel Security.* The first-year cost of purchasing equipment, hiring security officers, and preparing paperwork is approximately \$188 million. Following initial implementation, the annual cost is approximately \$144 million. Over the next 10 years, the cost would be PV \$1.1 billion approximately. The paperwork burden associated with planning would be approximately 140,000 hours in the first year and 7,000 hours in subsequent years.

- *Facility Security.* The first-year cost of purchasing equipment, hiring security officers, and preparing paperwork is an estimated \$963 million. Following initial implementation, the annual cost is approximately \$535 million. Over the next 10 years, the cost would be PV \$4.4 billion approximately. The paperwork burden associated with planning would be approximately 465,000 hours in the first year and 17,000 hours in subsequent years.

- *Port Security.* The first-year cost of establishing Port Security Committees and creating Port Security Plans for all port areas is an estimated \$120 million. The second-year cost is approximately \$106 million. In subsequent years, the annual cost is approximately \$46 million. Over the next 10 years, the cost would be PV \$477 million approximately. The paperwork burden associated with planning would be approximately 1,090,000 hours in 2003, 1,278,000 hours in 2004, and 827,000 hours in subsequent years.

Dated: December 20, 2002.

Paul J. Pluta,

Rear Admiral, U.S. Coast Guard, Assistant Commandant for Marine Safety, Security and Environmental Protection.

Appendix A: Maritime Security Issues for Discussion

General Security Provisions

1. *Obligations of Contracting Government with respect to security.* The SOLAS amendments (regulation 3) and ISPS Code (part A, section 4, and part B, paragraph 4) lay out a series of requirements for

Contracting Governments and Administrations to mandate security levels that are appropriate for their vessels and ports. The Coast Guard intends to implement these requirements in coordination with the Homeland Security Advisory System (HSAS). Homeland Security Presidential Directive (HSPD)-3 defines a five-tiered system for setting threat levels. We intend to implement Maritime Security (MARSEC) levels, which directly correspond to security levels as discussed in the SOLAS amendments and the ISPS Code. The MARSEC levels will be linked to the HSAS, as follows, to serve as the maritime sector's tool for communicating risk.

Homeland Security Advisory System (HSAS)	Maritime Security (MARSEC) Level
Low: Green	MARSEC Level 1.
Guarded: Blue	
Elevated: Yellow	
High: Orange	MARSEC Level 2.
Severe: Red	MARSEC Level 3.

We intend to communicate these MARSEC levels to our vessels and ports using such methods as Broadcast Notice to Mariners, community public alert systems, fax and e-mail alert lists, or other similar methods, and intend that these communication processes be addressed in the port security plan. To meet the SOLAS requirement to have a point of contact through which vessels and facilities can request advice or assistance or report any security concerns (chapter XI-2, regulation 7), we anticipate using the toll-free phone number of our National Response Center or a regional toll-free number as coordinated with other agencies. This number and point of contact information would be published in the Coast Pilot, on Web sites, and in other public information formats.

- From a port perspective, would these communication processes meet your needs? Why or why not?

- From a vessel perspective, would these communication processes meet your needs? Why or why not?

2. *Procedures for Authorizing a Recognized Security Organization.* The ISPS Code (part A, section 4, and part B, paragraph 4) allows Contracting Governments to delegate certain security related duties to Recognized Security Organizations (RSO). In order to ensure proper implementation at the outset of the MTSA as well as the international mandates, and because of the accelerated implementation timeline, the Coast Guard does not intend to delegate its authority to an RSO. However, in the future the Coast Guard may consider such delegation.

- Do you believe the Coast Guard should delegate its authority to an RSO keeping in mind the limitations in the ISPS Code (part A, section 4.3)?

- Do you believe there should be additional qualification and competency requirements to those listed in the ISPS Code part B, paragraph 4.5 for RSOs?

3. *Consideration of other Organizations competent in Maritime Security.* The Coast Guard recognizes that security assessments and plans for the maritime community may

require the assistance of organizations with maritime security competency. Currently there is not a standard for these organizations or companies; however, a benchmark has been established in the ISPS Code part B, paragraph 4.5.

- Should the Coast Guard formalize professional standards for companies or organizations that seek to do business providing guidance on vessel and facility security assessments and plans?

- Should the Coast Guard vet these organizations or are you aware of an alternative quality standard that should be associated with them?

4. *Procedures for Accepting Alternatives and Equivalencies.* The SOLAS amendments to chapter XI-2, regulation 11 and 12 along with part B, paragraph 4.26 and 4.27 of the ISPS Code allow Contracting Governments to permit alternatives and equivalencies to the security requirements if they are at least as effective as the mandates and are reported to the Organization. This concept aligns with traditional SOLAS language and provides for some flexibility in implementation. The Coast Guard intends to allow alternatives and equivalencies for vessels and some facilities, as appropriate. The Coast Guard would consider allowing a company that operates a number of similar vessels and terminals, to develop a master plan provided all aspects of the operation are addressed in lieu of individual plans as provided for in SOLAS chapter XI-2, regulation 11 and 12. Provisions for the submission of requests for the Coast Guard to consider alternatives or equivalencies will be similar to that already permitted in 46 CFR Subchapters, for example 46 CFR 30.15 or 70.15.

- Do you anticipate that your organization would request an alternative or equivalency? If so, why?

- Do you believe the submission format proposed by the Coast Guard is appropriate?

5. *Procedures for Accepting Industry Standards.* In addition to the equivalencies and alternative provisions discussed above, the Coast Guard is considering, for those vessels that are currently not required to meet SOLAS, accepting industry standards for security requirements to be used as an equivalent or alternative. To ensure security for our maritime community remains high, these standards would be reviewed and approved nationally. The Coast Guard also believes that in order to be deemed acceptable, compliance with an industry standard should be subject to verification by a third party audit procedure acceptable to the Coast Guard. The concept of this provision aligns with the current SOLAS provisions in chapter XI-2, regulations 11 and 12. The submission process will be similar to that found at 46 CFR 50.20-30, "alternative materials or methods of construction", whereby the proposed industrial standard will be submitted to the Commandant for review.

- Do you know of an industry standard that may be considered equivalent (or could be equivalent with revision) to the requirements of the SOLAS amendments and the ISPS Code?

- If an industry standard were available, would you consider implementing it? If so, why?

6. *Declaration of Security (DoS).* The ISPS Code (part A, section 5) requires Contracting Governments to determine when a DoS is required for vessels and facilities conducting vessel/port interface or vessel-to-vessel activities. A DoS is a document that establishes an agreement between a vessel and a facility, or between vessels, on their security arrangements to ensure their coordination and communication is clearly set out. At this time, the Coast Guard intends to issue national guidelines when a DoS must be executed, and the form of the DoS. The Coast Guard also intends to have each Port Security Committee determine the conditions for executing a DoS. Declarations of Security will be addressed in each Port Security Plan. In addition, the Port Security Committee will be asked to consider and include guidance in the Port Security Plan on what actions to take when vessels request a DoS or request to enter the Port with a security level higher than the Port's level. The ISPS Code also allows Administrations to give guidance on when their ships should request a DoS during a port call or when interacting with other vessels. The Coast Guard intends to issue this as guidance, either within regulations or as a separate document (NVIC), to assist ship owners in the development of their vessel security plans.

- During what operations or security levels do you believe a DoS would be appropriate to facilitate coordination of security measures between a facility and a vessel?

- What format, either regulation or guidance, would you prefer to assist you in developing your vessel security plan to address DoSs?

7. *Security of information contained in port, vessel and facility security assessments and plans.* The ISPS Code (part A, sections 9 and 16) and the MTSA (46 U.S.C. section 70101(d)) require documents related to security, especially security assessments and plans, to be kept in a manner that is protected from unauthorized access or disclosure. However, the Coast Guard will require access to vessel and facility records, as well as those held by other structures located on or adjacent to U.S. navigable waters, for the purpose of conducting or verifying assessments and plans. This information may be required to be provided upon request by the Coast Guard. The Coast Guard intends to require information related to Port Security, Vessel Security, and Facility Security Plans to be designated as Security Sensitive Information (SSI) in a manner similar to that used by the airline industry. Transportation Security Administration (TSA) is considering revisions to the SSI regulations (49 CFR part 1520) to enable this classification.

- Do you believe that a SSI classification will be sufficient? If not, why?

- Do you have a suggestion for an alternative way to protect this information yet allow approvals and review?

Port Security Provisions

8. *Port Security Plans and Committees.* The requirements for ports stem from the development of the new SOLAS amendments and the ISPS Code as well as the MTSA (46 U.S.C. sections 70103, 70104 and 70112). The

definition of port facilities is broad and covers all aspects of the interface between a ship and a facility, including anchorages and other areas typically considered by the United States as public waterways, as well as other structures located on or adjacent to U.S. navigable waters. Thus, the Coast Guard intends to invoke the alternative provided in part A, section 16.4 of the ISPS Code and combine facility plans with a port plan to encompass all of our U.S. navigable waters. The majority of the SOLAS amendments and ISPS Code requirements would be applied to U.S. facilities to ensure a seamless ship-to-facility security interface. However, the port security requirements will be the overarching instrument for implementing security communications and ensuring compliance. For U.S. purposes, the Port Facility Security Officer (PFSO) will be the Coast Guard Captain of the Port (COTP) who may require Facility Security Officers undertake certain responsibilities (such as signing a DoS), as outlined in the Port Security Plan (PSP). The Port Security Committees will assist the PFSO in developing the PSP and will be intimately involved in the exercises to ensure it remains effective. The Coast Guard intends to issue regulations that will lay out the Port Security Committees' and the PFSOs' responsibilities and guidance for the committee membership.

- Who do you believe should be involved in the Port Security Committees?

- Do you have a suggestion for how to ensure the involvement of the affected community listed in the section titled "Who should attend the public meetings?" of the notice?

9. *Port Security Assessments Requirement.* The Coast Guard is considering requirements for Port Security Assessments (PSAs), as discussed in ISPS Code part A, section 15 and part B paragraphs 15.1 through 15.16 as well as the MTSA (46 U.S.C. section 70102). The regulation also would contain a description of the role of Port Security Committees. Many assessments of this type have already been performed in ports and should be a good foundation for this requirement. Since the PSA will be integral in the development of the PSP, requirements for its update and review will also be included.

- Do you believe that your Port Security Committee, as described in the NVIC and above, is able to provide enough experience and expertise to develop PSAs? If no, why?
- Does your port currently have an assessment that you believe could be used for a PSA?

10. *Port security control of vessels, facilities, and operations.* The requirements for control of vessels are outlined in the SOLAS amendments, regulation XI-2/9, and the ISPS Code part B, paragraphs 4.29 through 4.46. The Coast Guard intends to implement control measures as detailed in the SOLAS amendments and ISPS Code requirements. The information from a vessel's advanced notice of arrival, which is being revised under a separate rulemaking, and other means of verifying compliance with the SOLAS amendments and ISPS Code, will provide our COTPs the ability to assess appropriate control measures for these

vessels. In addition, the Port Security Committee will be asked during the PSA process to review areas within the port, such as fleeting areas, regulated navigation areas, anchorages, and areas near facilities, to assess whether these areas should have security zones or patrol requirements established at certain security levels. If so, the Port Security Plan then would be required to address these security zones (or other security requirements) and arrangements to permanently establish the zones. Alternatively, such measures may be promulgated through regulation. The regulation would contain specific procedures for triggering security zone implementation through a broadcast notice to mariners or security level communication to the maritime community. Thus, mariners would know precisely what to expect in their waterways during higher security levels and facilities would also know if any operations would be restricted due to waterway concerns.

- Do you believe a system of waterway and facility restrictions pre-designated in regulations or other means (such as a Coast Pilot) would assist in your compliance with security requirements?

- Do you have any suggestions of other ways to restrict or control activities within the port area at higher security levels?

11. *Port security training and exercises.* Part A, section 18 and part B, paragraphs 18.1 through 18.6 of the ISPS Code detail training, drills, and exercise requirements for port facilities. To meet these requirements, the Coast Guard would require a quarterly exercise of the Port Security Plan. In addition, training requirements for Port personnel would also have to be included in the Port Security Plan. At this time, the Coast Guard does not expect to mandate a formal training course for port security personnel. However, at a minimum, facilities will have to ensure that security personnel receive appropriate training, consistent with part B of the ISPS Code, to ensure that they can carry out their assigned responsibilities. This includes, where appropriate, guidance on firearms safety. Drill requirements mandated for port security will be met in conjunction with drills for facility plans on a quarterly basis.

- Under this scheme, would you participate in a Port Security Plan exercise?

- Do you have a suggestion on a type of Port Security Plan exercise other than those listed in Part B, paragraph 18.6?

- Do you have a port personnel security training program or suggestions on training guidance for safety and security personnel?

Vessel Security Provisions

12. *Incorporation by Reference.* The Coast Guard is considering accepting national, State, and industry security standards to meet certain security requirement(s), as appropriate, such as a vessel security plan that incorporates the use of motion detection equipment that meets an accepted national standard.

- Do you know of a national, State, or industry standard that could be used in the marine environment?

- If a national, State, or industry standard was available, would you consider implementing it? If so, why?

13. *Obligations of the company.* The obligations and specific requirements of companies are discussed in SOLAS amendments (regulation 4 and 5) and the ISPS Code (part A, section 6 and part B, paragraphs 6.1 through 6.8). The Coast Guard would require Vessel Security Plans (VSPs) to describe how the company will meet its obligations and requirements.

- Do you believe that this adequately addresses the obligations and specific requirements of a company? If no, why?

- Do you have a suggestion for how to ensure that companies meet these obligations and requirements?

- What should the obligations of towing companies be with respect to the responsibility for barges?

14. *Vessel Security Requirements.* The SOLAS amendments (regulation 4) and ISPS Code (part A, section 7) require that vessels act upon security levels set by Contracting Governments through appropriate protective measures by carrying out certain specified activities (part A, section 7.2). The MTSA requires the Coast Guard to consider the types vessels that are likely to be involved in a transportation security incident. For the purposes of this notice and the Coast Guard discussion in Appendix C, cost impact was only developed for those vessels listed in NVIC 10-02 and also listed in the section titled, "Who should attend the public meetings?" The Coast Guard also recognizes that many other vessels could benefit from compliance with these requirements therefore, the Coast Guard is considering extending them to all vessels, including small passenger vessels or uninspected fishing vessels.

- Do you believe that the application of the requirements in part A, section 7-13 of the ISPS Code for the vessels indicated in the section titled "Who should attend the public meetings?" is appropriate? If not, why?

- Do you believe these security measures should apply to other vessels, not already listed?

- Do you believe that these activities and protective measures adequately address the security of a vessel? If no, why?

- Do you have a suggestion for appropriate security measures that a vessel can take to meet these requirements that are not already listed in part B, paragraphs 9.1 through 9.49?

15. *Vessel Security Assessments (VSA) Requirement.* The ISPS Code part A, section 8, and part B, paragraphs 8.1 through 8.14, as well as the MTSA (46 U.S.C. sections 70102 and 70166), require that a vessel perform a VSA that includes an on-scene security survey and provides details of those elements that the VSA will include. The VSA is integral in developing and updating the Vessel Security Plan. The Coast Guard would require VSAs for all vessels indicated in the section titled "Who should attend the public meetings?" of the notice. The Coast Guard would review these assessments when Vessel Security Plans are submitted for approval.

- Do you have any suggestions on how to best conduct a VSA and review results? Is there a current practice to meet this requirement?

- For vessels on domestic voyages, are there any appropriate alternatives to a VSA that could be considered?

16. *Vessel Security Plan (VSP)*

Requirement. The ISPS Code part A, section 9, and part B, paragraphs 9.1 through 9.53, as well as the MTSA (46 U.S.C. sections 70103 and 70104), require that VSPs be developed, taking into consideration the VSA, make provisions for the three MARSEC Levels, and be reviewed and updated. The Coast Guard's requirements would incorporate all of these elements and would also provide an outline that the VSP would follow or be cross-referenced using a similar approach as done in 33 CFR 155.1030.

- Do you have any suggestions on additional items the VSP should address?
- Do you have a suggestion or a best practice to meet this VSP requirement?
- Would you find an outline a valuable aid to meeting these requirements? If not, why?

17. *Submission of Vessel Security Plans for approval.* The ISPS Code (part A, section 9) requires that vessels carry on board a VSP that is approved by the Administration. The MTSA further requires VSPs to be approved by the Secretary. Therefore, for foreign vessels required to comply with SOLAS, the Coast Guard will deem Flag state approval of a VSP that meets the requirements of SOLAS and the ISPS Code to be approval of the Secretary for purposes of the MTSA. The Coast Guard would approve all other VSPs at the Marine Safety Center or at the COTP level, depending on the class of vessel. The submission format would be similar to that already required in 33 CFR 120.305. In addition, for efficiency and timeliness, the Coast Guard is considering alternative methods of Coast Guard approval for VSPs for certain vessels that operate on domestic voyages. One possible alternative includes Coast Guard approval of a unified or corporate plan that would be implemented on a similarly situated fleet of vessels in common ownership. Another alternative could include verification of implementation of a pre-approved security plan for a particular segment of industry.

- Do you have suggestions on how these approvals could be streamlined? Is there an alternative process?
- Do you believe the submission format proposed by the Coast Guard is appropriate?

18. *Existing Security Measures for Certain Vessels.* The Coast Guard is evaluating the need for retaining certain security measures in existing regulations, 33 CFR part 120, for those vessels (e.g., large passenger vessels) that could be involved in a transportation security incident that results in a catastrophic loss of life. The Coast Guard considers that 33 CFR part 120 meets the requirements of the SOLAS amendments and the ISPS Code.

- Do you believe that additional security requirements are needed for certain vessel types? If so, why and what would those requirements be?

19. *Vessel Security Recordkeeping.* The ISPS Code part A, section 10, and part B, paragraphs 10.1 and 10.2, require certain security records to be kept on board the vessel and retained for a period specified by the Administration. The Coast Guard would require all vessels to keep these records for at least 2 years and make them available for review during inspections or boardings.

Presently, there are no requirements for the format of these records. However, their review would have to provide an inspector with the appropriate information to ensure the vessel's security plan is properly implemented. The Coast Guard does not intend to prescribe where these records are kept nor their format.

- Do you have a suggestion or best practice related to recordkeeping you believe the Coast Guard should require?

- Do you wish the Coast Guard to prescribe a format for these records?

20. *Company Security Officer Designation.* The ISPS Code (part A, section 11) as well as the MTSA (46 U.S.C. section 70103), specify that the Company must designate a Company Security Officer (CSO) and details their duties, responsibilities, and competencies (part A, sections 13.1 and 13.5 and part B, paragraph 13.1). In addition, CSOs are required to participate in security exercises as discussed in part B, paragraph 13.7 of the ISPS Code. The Coast Guard intends to include these requirements for all vessels indicated in the section titled "Who should attend the public meetings?" The Coast Guard recognizes that many security programs are already in place and have personnel working in the maritime community with the experience and the competencies reflected in the ISPS Code. At this time, the Coast Guard does not intend to certify courses as meeting the standards of the ISPS Code or require any type of license for a CSO. Rather, the Coast Guard intends to accept Company certification for these officers indicating that they have the knowledge, experience and competencies as required by the ISPS Code. The Coast Guard also intends to have CSOs or Companies provide proof that CSOs have participated in annual exercises, and records of that participation would have to be retained for 2 years.

- Do you believe the Coast Guard should require CSOs to attend training?
- Do you believe Company certification is appropriate or do you have a suggestion for an alternate verification for the CSO qualifications?
- Do you believe proof of participation in annual exercises should be retained for 2 years? If not, how long? Why?

21. *Vessel Security Officer Designation.* The ISPS Code (part A, section 11) as well as the MTSA (46 U.S.C. section 70103), specify that each vessel shall designate a Vessel Security Officer (VSO) and details their duties, responsibilities, and competencies (part A, section 13.2 and part B, paragraphs 13.1 and 13.2). In addition, VSOs are required to participate, if available, in security exercises as discussed in part B, paragraph 13.7 of the ISPS Code. Since many security programs and personnel are already working in the maritime community and have the competencies reflected in the ISPS Code, at this time, the Coast Guard does not intend to certify courses as meeting the standards of the ISPS Code or require any type of license for a VSO. Rather, the Coast Guard intends to accept Company certification for these officers indicating that they have the knowledge, experience and competencies as required by the ISPS Code.

The Coast Guard is also considering alternatives for some vessel classes, such as barges, to allow a Company Security Officer in lieu of a VSO with duties that encompass both. It should be noted that there is no prohibition to the master also being designated as the VSO although on large vessels, this may be impractical.

- Do you believe the Coast Guard should require VSOs to attend formal training?
- Do you believe Company certification is appropriate or do you have a suggestion for an alternate verification for the VSO qualifications?
- Do you have any suggestions for certain classes of vessels being allowed an alternative to a VSO? If so, how or who would you make responsible for the VSO duties?

22. *Security training and drill requirements for vessel personnel.* The ISPS Code (part A, sections 13.3 and 13.4, and part B, paragraph 13.3) as well as section 109 of the MTSA, specify that vessel personnel having specific security duties and responsibilities be trained in their duties and have the knowledge needed to carry them out. Part B, paragraph 13.4 also requires a basic security knowledge and competency for all personnel employed on the vessel to ensure security awareness. In addition, vessel personnel are required to participate in security drills as discussed in part A, section 13.4, and part B, paragraphs 13.5 and 13.6 of the ISPS Code. The Coast Guard intends to allow vessel masters, VSOs, or CSOs to certify that vessel personnel have received the training required to fulfill their security duties, if applicable or the general security awareness training required for all personnel. A record (such as a training record) kept on board the vessel or any other form of acknowledgment (such as a log entry) would be sufficient for this purpose. A record of drills would also be required and is discussed in paragraph number 19 of this appendix.

- Do you believe the Coast Guard should require vessel personnel to attend formal training?
- Do you believe prescribing the format for training records would assist you in meeting these requirements?

23. *Certification for vessels.* The ISPS Code, parts A and B, section 19, requires Administrations to verify and certify by issuing an International Ship Security Certificate (ISSC) that those vessels subject to SOLAS comply with the applicable requirements of SOLAS chapter XI-2 and the ISPS Code. The Coast Guard intends to amend 46 CFR 2.01-25 by adding new paragraph (a)(viii) referring to ISSC. Compliance with regulations for domestic vessels will be verified during issuance and renewal of Certification of Inspection. Issuance or endorsement of the Certificate of Inspection (COI) would be contingent upon a vessel's compliance with these regulations. Vessels that are not required to be inspected by the Coast Guard under title 46 of the U.S.C., would be required to have proof on board the vessel certifying that the vessel meets these requirements and that they are implementing their VSP.

- Do you have any other suggestions for verification and certification that vessels comply with security regulations?

Facility Security Provisions

24. *Incorporation by Reference.* The Coast Guard is considering accepting national, State, and industry security standards to meet certain security requirement(s), as appropriate, e.g., a facility security plan that incorporates lighting or fencing equipment that meets an accepted national standard.

- Do you know of a national, state, and industry standard that could be used in the marine environment?
- If a national, state, and industry standard were available, would you consider implementing it? If so, why?

25. *Facility Security Requirement.* The SOLAS amendments (chapter XI-2, regulation 10) and ISPS Code parts A and B, section 14 require that facilities act upon security levels set by Contracting Governments through appropriate protective measures by carrying out certain specified activities (part A, section 14.2). The MTSA requires the Coast Guard to consider the types facilities that are likely to be involved in a transportation security incident. For the purposes of this notice and the Coast Guard discussion in Appendix C, cost impact was only developed for those facilities listed in NVIC 11-02 and also listed in the section titled, "Who should attend the public meetings?" The Coast Guard also recognizes that many other facilities could benefit from compliance with these requirements therefore, the Coast Guard is considering extending them to all facilities, including dry bulk or general cargo facilities or ship repair facilities.

- Do you believe that the application of the requirements in part A, section 14-18 of the ISPS Code for the facilities indicated in the section titled "Who should attend the public meetings?" is appropriate? If not, why?
- Do you believe these security measures should apply to other facilities, not already listed?
- Do you believe that these activities and protective measures adequately address the security of a facility? If no, why?
- Do you have a suggestion for appropriate security measures that a facility can take to meet these requirements that are not already listed in part B, paragraphs 16.1 through 16.63?

26. *Facility Security Assessments (FSA) Requirement.* The ISPS Code parts A and B, section 15, as well as the MTSA (46 U.S.C. sections 70102 and 70116), require that a facility perform a FSA that includes an on-scene security survey and provides details of those elements that the FSA will include. The FSA is integral in developing and updating the Facility Security Plan. The Coast Guard is considering requiring FSAs for all facilities indicated in the section titled "Who should attend the public meetings?" of the notice. The Coast Guard intends to review these assessments when Facility Security Plans are submitted for approval.

- Do you have any suggestions on how to best conduct a FSA and review the results? Is there a current practice to meet this requirement?
- Are there any appropriate alternatives to a FSA that could be considered?

27. *Facility Security Plans.* The ISPS Code parts A and B, section 16, as well as the

MTSA (46 U.S.C. sections 70103 and 70104), require that FSPs be developed taking into consideration the facility security assessment, make provisions for the three MARSEC Levels, and be reviewed and updated. The Coast Guard is considering requirements that incorporate all of these requirements and also would provide an outline for the FSP. The outline would follow or be cross-referenced using a similar approach as done in 33 CFR part 155.1030.

- Do you have any suggestions on additional items the FSP should address?
- Do you have a suggestion or a best practice to meet this FSP requirement?
- Would you find an outline a valuable aid to meeting these requirements? If not, why?

28. *Submission of Facility Security Plans for approval.* The ISPS Code (part A, section 16) requires facilities to develop and maintain a facility security plan (FSP) that is approved by the Contracting Government in whose territory the facility is located. The Coast Guard intends to review and approve FSPs at the COTP level. The submission format would be similar to that already required in 33 CFR 120.305. The Coast Guard is considering the submission of a single FSP for companies that own and operate both the facility and vessels that call on that facility.

- Do you have suggestions on how these approvals could be streamlined or an alternative process?
 - Do you believe the submission format proposed by the Coast Guard is appropriate?
29. *Facility Security Recordkeeping.* Although records for facilities are not specifically addressed in the ISPS Code, the Coast Guard intends to require certain security records be kept for certain security related activities and incidents and retained for a period specified by the Coast Guard. The Coast Guard would require these records to be kept for at least 2 years and will review them during inspections. Presently, there are no requirements for the format of these records. However, their review would have to provide an inspector with the appropriate information to ensure the facility's security plan is properly implemented. The Coast Guard does not intend to prescribe where these records are kept nor their format.

- Do you have a suggestion or best practice related to recordkeeping you believe the Coast Guard should require?
- Do you wish the Coast Guard to prescribe a format for these records?

30. *Facility Security Officer.* The ISPS Code, parts A and B, section 17, as well as the MTSA (46 U.S.C. section 70103), specify that the each facility shall designate a Facility Security Officer (FSO) and details their duties, responsibilities, and competencies (part A, section 17.2 and part B, paragraphs 17.1 and 17.2). In addition, FSOs are required to participate in security exercises as discussed in part B, paragraph 18.6 of the ISPS Code. Since many security programs and personnel are already working in the maritime community and have the competencies reflected in the ISPS Code, at this time, the Coast Guard does not intend to certify courses as meeting the standards of the ISPS Code or require any type of license for a FSO. Rather, the Coast Guard intends to accept Company certification for these

officers indicating that they have the knowledge, experience and competencies as required by the ISPS Code. It should be noted that there is no prohibition of the FSO having a collateral duty provided the individual is able to perform the duties and responsibilities required by the ISPS Code and the approved FSP.

- Do you believe the Coast Guard should require FSOs to attend training?
- Do you believe Company certification is appropriate or do you have a suggestion for an alternate verification for the FSO qualifications?
- Would there be a case where a FSO may perform their duties for more than one facility?
- Do you believe proof of participation in annual exercises should be retained for 2 years? If not, how long? Why?

31. *Training, drills and exercises on Facility Security.* The ISPS Code, parts A and B, section 18, as well as section 109 of the MTSA, specify that facility personnel having specific security duties and responsibilities be trained in their duties and have the knowledge needed to carry them out. Part B, paragraph 18.3 also requires a basic security knowledge and competency for all personnel employed at the facility to ensure security awareness. In addition, facility personnel are required to participate in security drills as discussed in part A, section 18 and part B, paragraphs 18.4 and 18.6 of the ISPS Code. The Coast Guard intends to allow FSOs to certify that facility personnel have received the training required to fulfill their security duties, if applicable or the general security awareness training required for all personnel. A record (e.g., a training record) kept or any other form of acknowledgment (e.g., a log entry) would be sufficient for this purpose. A record of drills would also be required and is discussed in item number 28 of this notice.

- Do you believe the Coast Guard should require facility personnel to attend training?
- Do you believe prescribing the format for training records would assist you in meeting these requirements?

32. *Certification for facilities.* The ISPS Code does not specifically require that each facility be certified. The Coast Guard would review and approve the FSP and would require companies to certify their compliance with these requirements and that each facility has drafted and implemented an FSP. The Coast Guard would inspect facilities to verify compliance.

- Do you have any suggestions for verification and certification that facilities comply with security regulations?
- Do you believe the Coast Guard should allow companies to certify their facilities?

Other Security Provisions

33. *Permanent hull marking requirement.* The SOLAS amendments created a new regulation in chapter XI-1 (regulation 3) that requires vessels to have their identification number permanently marked on their hull and in an easily accessible place on the transverse bulkhead of the machinery space or on another suitable interior location, as specified. At this time, the Coast Guard does not intend to extend the application of this requirement to vessels limited to domestic

voyages. However, all vessels subject to SOLAS and conducting international voyages, including towing vessels and offshore supply vessels whose international tonnage is greater than 300 gross tons (gt), would be required to comply with this regulation when the SOLAS amendments enter into force.

- Do you believe the Coast Guard should extend this requirement to vessels limited to domestic voyages? If so, why?

34. Continuous Synopsis Record requirement. The SOLAS amendments created a new regulation in chapter XI-1 (regulation 5) that requires vessels to maintain and update a Continuous Synopsis Record, to be kept on board, that contains information such as the name of the flag Administration, the date of the vessel's registry, the vessel's identification number, *etc.* At this time, the Coast Guard does not intend to extend the application of this requirement to vessels limited to domestic voyages. However, all vessels subject to SOLAS and conducting international voyages, including towing vessels and offshore supply vessels whose international tonnage is greater than 500 gt would be required to comply with this regulation when the SOLAS amendments enter into force.

- Do you believe the Coast Guard should extend this requirement to vessels limited to domestic voyages? If so, why?

35. Security alert system requirement. The SOLAS amendments created a new regulation in chapter XI-2 (regulation 6) that requires vessels to have a security alert system. For the purposes of this notice and the Coast Guard discussion in Appendix C, cost impact was only developed for this requirement to those vessels required to meet SOLAS chapter XI-2. However, the Coast Guard is considering applying the requirement to vessels limited to domestic voyages that are engaged in the transport of certain dangerous cargoes. The Coast Guard also recognizes that many other vessels could benefit from compliance with this requirement such as certain passenger vessels or towing vessels.

- Do you believe this requirement would benefit vessels limited to domestic voyages engaged in the transport of certain dangerous cargoes?

- Do you believe the Coast Guard should extend this requirement to other vessels limited to domestic voyages? If so, why?

36. Fixed and floating platforms requirements. The International Maritime Organization issued a resolution titled, "Establishment of Appropriate Measures to Enhance the Security of Ships, Port Facilities, Mobile Offshore Drilling Units on Location and Fixed and Floating Platforms Not Covered by Chapter XI-2 of the 1974 SOLAS Convention" which was adopted by the Conference on Maritime Security as Resolution 7 on December 12, 2002. This resolution encourages Contracting Governments to consider security requirements for these maritime operators and platforms. The Coast Guard is considering including these entities in its Port Security Plan regime. We are also working with the offshore industry to develop security standards that would

provide a level of security equivalent to that being established for land based facilities, yet tailored to the unique offshore operating environment. Once acceptable offshore industry security standards are determined, such standards may be incorporated into regulations as part of a separate rulemaking procedure.

- Do you believe the Coast Guard should extend security requirements to offshore platforms? If so, why?

37. Seafarers' identification criteria requirements. The MTSA (46 U.S.C. section 70111) requires the Secretary to establish enhanced crewmember identification. In addition, section 103 of the MTSA encourages the Secretary to negotiate an agreement for an international system of identification for seafarers. In March 2002, the Governing Body of the International Labour Organization (ILO) agreed to have the International Labour Conference consider amendments to the Seafarers' Identity Documents Convention, 1958 (No. 108) regarding seafarer identification at its 91st session in June 2003. In support of this effort, the International Maritime Organization issued a resolution titled, "Enhancement of Security in Co-operation with the International Labour Organization" which was adopted by the Conference on Maritime Security as Resolution 8 on December 12, 2002. The Coast Guard has been working with the Immigration and Naturalization Service, Department of State, Maritime Administration, TSA, and others to support the work of ILO. The U.S. intends to await the outcome of the June 2003 ILO conference prior to developing further seafarer identification domestic policy.

In addition to the above, the MTSA (46 U.S.C. section 70105) requires the Secretary to develop and implement a Transportation Security Card to control access to secure areas on a vessel or facility. The U.S. is moving this requirement forward through its work on a Transportation Worker Identification Credential System (TWIC). Pilot testing of the TWIC is scheduled for one east regional and one west regional port, each in communication with a TSA central control point. This pilot project allows the TSA to leverage key regional stakeholders and analyze life cycle and cost benefits, as well as the performance of various forms of identification technologies.

Recognizing that the implementation of the TWIC and the ILO efforts on seafarers identification involve substantial negotiation and development, the Coast Guard therefore intends to continue its use of the criteria it set out in its clarification of regulations notice entitled "Maritime Identification Credentials" published in the **Federal Register** (67 FR 51082, August 7, 2002). This document can be viewed on the DOT Document Management System at <http://dms.dot.gov> under Docket# USCG-2002-12917.

- Do you believe the Coast Guard should amend its policy notice to capture additional forms of identification? If so, why?

38. Advanced notice of arrival (ANOVA) requirements. The Coast Guard has a notice of proposed rulemaking entitled "Notification of Arrival in U.S. Ports"

published in the **Federal Register** (67 FR 41659, June 19, 2002). This document can be viewed on the DOT Document Management System at <http://dms.dot.gov> under Docket # USCG-2002-11865-1. The comment period for that rulemaking has closed. The Coast Guard does not intend to add any additional notification requirements to that rulemaking.

However, the SOLAS amendments and the ISPS Code contain several information-related requirements that are not currently part of the ANOVA. The Coast Guard is considering expanding its advanced notice of arrival information to incorporate these new international requirements (SOLAS chapter XI-2, regulation 9). We are also considering requiring foreign flag vessels to provide advance notification on their compliance with part B of the ISPS Code. In addition, the Coast Guard is considering further expanding the notice requirements on the Mississippi River and its tributaries above mile marker 235 for certain barges carrying certain dangerous cargoes.

- Having reviewed the SOLAS amendments and the ISPS Code, what additional information do you believe should be provided by vessels prior to entering our ports?

- Do you believe further ANOVA requirements are appropriate for the Mississippi River and its tributaries above mile marker 235?

39. Foreign Port Assessments. Section 102 of the MTSA (46 U.S.C. section 70108) requires the Secretary to assess the effectiveness of antiterrorism measures maintained at a foreign port that serves vessels departing on a voyage to the U.S. or any other port that the Secretary believes poses a security risk to international maritime commerce. In general, the Coast Guard intends to accept a foreign government's approval of the respective port facility security plans, thereby attesting to their compliance with SOLAS and the ISPS Code, to provide the initial assessment of that foreign port's antiterrorism security. However, the Coast Guard in making assessments under the MTSA will also consider any other relevant information and possibly conduct audits. No regulations are required to implement this provision of the MTSA because these assessments are an internal deliberative matter and further related to foreign relations. However, the Coast Guard would appreciate public comment on the following:

- Should the Coast Guard accept approval of foreign port facility security plans as a preliminary indication that the foreign port is maintaining effective antiterrorism measures?

- What factors do you believe the Coast Guard should consider in assessing the effectiveness of antiterrorism measures at foreign ports?

40. Automatic Identification System (AIS) requirements. Regulation V/19 of SOLAS sets forth the international requirements for the carriage of automatic identification systems (AIS), including an implementation schedule that was recently accelerated by the newly adopted amendments to SOLAS. Domestically, section 102 of the MTSA (46 U.S.C. section 70114) gives the Secretary additional broad discretion to require AIS on

any vessel operating on the navigable waters of the United States if necessary for the safety of navigation. In this regard, the Coast Guard considers that requiring AIS for security purposes is an essential element in ensuring the safety of navigation. At a minimum, the MTSA specifically requires the following vessels to have AIS:

- (a) A self-propelled commercial vessel of at least 65 feet overall in length;
- (b) A vessel carrying more than a number of passengers for hire determined by the Secretary;
- (c) A towing vessel of more than 26 feet overall in length and 600 horsepower;
- (d) Any other vessel for which the Secretary decides that an automatic identification system is necessary for the safe navigation of the vessel.

The Secretary may exempt or waive any such vessel from this requirement if AIS is not necessary for the safety of navigation. The implementation dates for AIS in the MTSA align with the SOLAS requirements.

As reflected in the Department of Transportation's Fall 2002 Unified Agenda (67 FR 74853, December 9, 2002), a separate AIS notice of proposed rulemaking should be published in the near future. Therefore, it is not the Coast Guard's intent to interfere with that rulemaking. However, because recent events indicate that smaller vessels may be used as weapons against maritime transportation, the Coast Guard is requesting limited public comment related to the MTSA requirements as follows:

- Should any of the vessels listed in the MTSA be exempted from carrying AIS because no security benefit would be derived from such a requirement?
- Beyond the SOLAS requirements and the vessels specifically listed in the MTSA, what other vessels should be required to carry AIS for security purposes?
- Are there any particular navigable waters of the U.S. where the AIS carriage requirement should be waived because no security benefit would be derived from the requirement?

Preliminary Cost Analysis

The Coast Guard is seeking public comment on the following assumptions used in the preliminary cost analysis:

- The loaded cost of a full-time employee designated to be the Company Security Officer or a Facility Security Officer would be \$150,000 per year.
- Some vessel and facility owners would designate the Company Security Officer and Facility Security Officer duties to an existing employee, and these collateral duties would take about 25 percent of the employee's time.
- Security functions aboard vessels would not require additional manning.
- Security functions for facilities would require additional security guards with a loaded rate of \$40,000 per year.
- The types of equipment vessels or facilities would install are an accurate representation of the equipment needs owners and operators can expect to face.

In addition, we are seeking public comment on the costs vessel and facility owners or operators would incur in the event MARSEC levels 2 or 3 are implemented.

Finally, we are seeking public comment on how these requirements will economically impact small businesses, Indian tribal governments, as well as comment on anticipated energy impacts.

Appendix B—SOLAS Amendments and ISPS Code

Note: The text in this appendix is excerpted from IMO documents SOLAS/CONF.5/DC/1, SOLAS/CONF.5/DC/2, and SOLAS/CONF.5/DC/2/Add.1, and has been edited to reflect the final decisions and other editorial corrections reflected in SOLAS/CONF.5/33.

Amendments to the International Convention for the Safety of Life at Sea, 1974 as Amended

Chapter V—Safety of Navigation

Regulation 19—Carriage Requirements for Shipborne Navigational Systems and Equipment

1 The existing subparagraphs .4, .5 and .6 of paragraph 2.4.2 are replaced by the following:

“4 In the case of ships, other than passenger ships and tankers, of 300 gross tonnage and upwards but less than 50,000 gross tonnage, not later than the first safety equipment survey¹ after 1 July 2004 or by 31 December 2004, whichever occurs earlier; and”

2 The following new sentence is added at the end of the existing subparagraph .7 of paragraph 2.4:

“Ships fitted with AIS shall maintain AIS in operation at all times except where international agreements, rules or standards provide for the protection of navigational information.”

Chapter XI—Special Measures to Enhance Maritime Safety

3 The existing chapter XI is renumbered as chapter XI-1.

Regulation 3—Ship identification number 4 The following text is inserted after the title of the regulation:

“(Paragraphs 4 and 5 apply to all ships to which this regulation applies. For ships constructed before 1 July 2004, the requirements of paragraphs 4 and 5 shall be complied with not later than the first scheduled dry-docking of the ship after 1 July 2004.)”

5 The existing paragraph 4 is deleted and the following new text is inserted:

“4 The ship's identification number shall be permanently marked:

.1 In a visible place either on the stern of the ship or on either side of the hull, amidships port and starboard, above the deepest assigned load line or either side of the superstructure, port and starboard or on the front of the superstructure or, in the case of passenger ships, on a horizontal surface visible from the air; and

.2 In an easily accessible place either on one of the end transverse bulkheads of the machinery spaces, as defined in regulation II-2/3.30, or on one of the hatchways or, in the case of tankers, in the pump-room or, in the case of ships with ro-ro spaces, as defined in regulation II-2/3.41, on one of the end transverse bulkheads of the ro-ro spaces.

5.1 The permanent marking shall be plainly visible, clear of any other markings on the hull and shall be painted in a contrasting colour.

5.2 The permanent marking referred to in paragraph 4.1 shall be not less than 200 mm in height. The permanent marking referred to in paragraph 4.2 shall not be less than 100 mm in height. The width of the marks shall be proportionate to the height.

5.3 The permanent marking may be made by raised lettering or by cutting it in or by centre punching it or by any other equivalent method of marking the ship identification number which ensures that the marking is not easily expunged.

5.4 On ships constructed of material other than steel or metal, the Administration shall approve the method of marking the ship identification number.”

6 The following new regulation 5 is added after the existing regulation 4:

Regulation 5—Continuous Synopsis Record

1 Every ship to which chapter I applies shall be issued with a Continuous Synopsis Record.

2.1 The Continuous Synopsis Record is intended to provide an on-board record of the history of the ship with respect to the information recorded therein.

2.2 For ships constructed before July 1, 2004, the Continuous Synopsis Record shall, at least, provide the history of the ship as from July 1, 2004.

3 The Continuous Synopsis Record shall be issued by the Administration to each ship that is entitled to fly its flag and it shall contain at least, the following information:

.1 The name of the State whose flag the ship is entitled to fly;

.2 The date on which the ship was registered with that State;

.3 The ship's identification number in accordance with regulation 3;

.4 The name of the ship;

.5 The port at which the ship is registered;

.6 The name of the registered owner(s) and their registered address(es);

.7 The name of the registered bareboat charterer(s) and their registered address(es), if applicable;

.8 The name of the Company, as defined in regulation IX/1, its registered address and the address(es) from where it carries out the safety management activities;

.9 The name of all classification society(ies) with which the ship is classed;

.10 The name of the Administration or of the Contracting Government or of the recognized organization which has issued the Document of Compliance (or the Interim Document of Compliance), specified in the ISM Code as defined in regulation IX/1, to the Company operating the ship and the name of the body which has carried out the audit on the basis of which the document

¹The first safety equipment survey means the first annual survey, the first periodical survey or the first renewal survey for safety equipment, whichever is due first after July 1, 2004 and, in addition, in the case of ships under construction, the initial survey.

was issued, if other than that issuing the document;

.11 The name of the Administration or of the Contracting Government or of the recognized organization that has issued the Safety Management Certificate (or the Interim Safety Management Certificate), specified in the ISM Code as defined in regulation IX/1, to the ship and the name of the body which has carried out the audit on the basis of which the certificate was issued, if other than that issuing the certificate;

.12 The name of the Administration or of the Contracting Government or of the recognized security organization that has issued the International Ship Security Certificate (or an Interim International Ship Security Certificate), specified in part A of the ISPS Code as defined in regulation XI-2/1, to the ship and the name of the body which has carried out the verification on the basis of which the certificate was issued, if other than that issuing the certificate; and

.13 The date on which the ship ceased to be registered with that State.

4.1 Any changes relating to the entries referred to in paragraphs 3.4 to 3.12 shall be recorded in the Continuous Synopsis Record so as to provide updated and current information together with the history of the changes.

4.2 In case of any changes relating to the entries referred to in paragraph 4.1, the Administration shall issue, as soon as is practically possible but not later than three months from the date of the change, to the ships entitled to fly its flag either a revised and updated version of the Continuous Synopsis Record or appropriate amendments thereto.

4.3 In case of any changes relating to the entries referred to in paragraph 4.1, the Administration, pending the issue of a revised and updated version of the Continuous Synopsis Record, shall authorise and require either the Company as defined in regulation IX/1 or the master of the ship to amend the Continuous Synopsis Record to reflect the changes. In such cases, after the Continuous Synopsis Record has been amended the Company shall, without delay, inform the Administration accordingly.

5.1 The Continuous Synopsis Record shall be in English, French or Spanish language. Additionally, a translation of the Continuous Synopsis Record into the official language or languages of the Administration may be provided.

5.2 The Continuous Synopsis Record shall be in the format developed by the Organization and shall be maintained in accordance with guidelines developed by the Organization. Any previous entries in the Continuous Synopsis Record shall not be modified, deleted or, in any way, erased or defaced.

6 Whenever a ship is transferred to the flag of another State or the ship is sold to another owner (or is taken over by another bareboat charterer) or another Company assumes the responsibility for the operation of the ship, the Continuous Synopsis Record shall be left on board.

7 When a ship is to be transferred to the flag of another State, the Company shall notify the Administration of the name of the

State under whose flag the ship is to be transferred so as to enable the Administration to forward to that State a copy of the Continuous Synopsis Record covering the period during which the ship was under their jurisdiction.

8 When a ship is transferred to the flag of another State the Government of which is a Contracting Government, the Contracting Government of the State whose flag the ship was flying hitherto shall transmit to the Administration as soon as possible after the transfer takes place a copy of the relevant Continuous Synopsis Record covering the period during which the ship was under their jurisdiction together with any Continuous Synopsis Records previous issued to the ship by other States.

9 When a ship is transferred to the flag of another State, the Administration shall append the previous Continuous Synopsis Records to the Continuous Synopsis Record the Administration will issue to the ship so to provide the continuous history record intended by this regulation.

10 The Continuous Synopsis Record shall be kept on board the ship and shall be available for inspection at all times."

7 The following new chapter XI-2 is inserted after the renumbered chapter XI-1:

Chapter XI-2—Special Measures to Enhance Maritime Security

Regulation 1—Definitions

1 For the purpose of this chapter, unless expressly provided otherwise:

.1 Bulk carrier means a bulk carrier as defined in regulation IX/1.6.

.2 Chemical tanker means a chemical tanker as defined in regulation VII/8.2.

.3 Gas carrier means a gas carrier as defined in regulation VII/11.2.

.4 High-speed craft means a craft as defined in regulation X/1.2.

.5 Mobile offshore drilling unit means a mechanically propelled mobile offshore drilling unit, as defined in regulation IX/1, not on location.

.6 Oil tanker means an oil tanker as defined in regulation II-1/2.12.

.7 Company means a Company as defined in regulation IX/1.

.8 Ship/port interface means the interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons, goods or the provisions of port services to or from the ship.

.9 Port facility is a location, as determined by the Contracting Government or by the Designated Authority, where the ship/port interface takes place. This includes areas such as anchorages, waiting berths and approaches from seaward, as appropriate.

.10 Ship to ship activity means any activity not related to a port facility that involves the transfer of goods or persons from one ship to another.

.11 Designated Authority means the organization(s) or the administration(s) identified, within the Contracting Government, as responsible for ensuring the implementation of the provisions of this chapter pertaining to port facility security and ship/port interface, from the point of view of the port facility.

.12 International Ship and Port Facility Security (ISPS) Code means the International Code for the Security of Ships and of Port Facilities consisting of part A (the provisions of which shall be treated as mandatory) and part B (the provisions of which shall be treated as recommendatory), as adopted, on December 12, 2002, by resolution 2 of the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 as may be amended by the Organization, provided that:

.1 Amendments to part A of the Code are adopted, brought into force and take effect in accordance with article VIII of the present Convention concerning the amendment procedures applicable to the Annex other than chapter I; and

.2 Amendments to part B of the Code are adopted by the Maritime Safety Committee in accordance with its Rules of Procedure.

.13 Security incident means any suspicious act or circumstance threatening the security of a ship, including a mobile offshore drilling unit and a high speed craft, or of a port facility or of any ship/port interface or any ship to ship activity.

.14 Security level means the qualification of the degree of risk that a security incident will be attempted or will occur.

.15 Declaration of security means an agreement reached between a ship and either a port facility or another ship with which it interfaces specifying the security measures each will implement.

.16 Recognized security organization means an organization with appropriate expertise in security matters and with appropriate knowledge of ship and port operations authorized to carry out an assessment, or a verification, or an approval or a certification activity, required by this chapter or by part A of the ISPS Code.

2 The term "ship", when used in regulations 3 to 13, includes mobile offshore drilling units and high-speed craft.

3 The term "all ships", when used in this chapter, means any ship to which this chapter applies.

4 The term "Contracting Government", when used in regulations 3, 4, 7, and 10 to 13, includes a reference to the "Designated Authority".

Regulation 2—Application

1 This chapter applies to:

.1 The following types of ships engaged on international voyages:

.1.1 Passenger ships, including high-speed passenger craft;

.1.2 Cargo ships, including high-speed craft, of 500 gross tonnage and upwards; and

.1.3 Mobile offshore drilling units; and

.2 Port facilities serving such ships engaged on international voyages.

.2 Notwithstanding the provisions of paragraph 1.2, Contracting Governments shall decide the extent of application of this chapter and of the relevant sections of part A of the ISPS Code to those port facilities within their territory which, although used primarily by ships not engaged on international voyages, are required, occasionally, to serve ships arriving or departing on an international voyage.

2.1 Contracting Governments shall base their decisions, under paragraph 2, on a port

facility security assessment carried out in accordance with the provisions of part A of the ISPS Code.

2.2 Any decision which a Contracting Government makes, under paragraph 2, shall not compromise the level of security intended to be achieved by this chapter or by part A of the ISPS Code.

3 This chapter does not apply to warships, naval auxiliaries or other ships owned or operated by a Contracting Government and used only on Government non-commercial service.

4 Nothing in this chapter shall prejudice the rights or obligations of States under international law.

Regulation 3—Obligations of Contracting Governments With Respect to Security

1 Administrations shall set security levels and ensure the provision of security level information to ships entitled to fly their flag. When changes in security level occur, security level information shall be updated as the circumstance dictates.

2 Contracting Governments shall set security levels and ensure the provision of security level information to port facilities within their territory, and to ships prior to entering a port, or whilst in a port, within their territory. When changes in security level occur, security level information shall be updated as the circumstance dictates.

Regulation 4—Requirements for Companies and Ships

1 Companies shall comply with the relevant requirements of this chapter and of part A of the ISPS Code, taking into account the guidance given in part B of the ISPS Code.

2 Ships shall comply with the relevant requirements of this chapter and of part A of the ISPS Code, taking into account the guidance given in part B of the ISPS Code, and such compliance shall be verified and certified as provided for in part A of the ISPS Code.

3 Prior to entering a port, or whilst in a port, within the territory of a Contracting Government, a ship shall comply with the requirements for the security level set by that Contracting Government, if such security level is higher than the security level set by the Administration for that ship.

4 Ships shall respond without undue delay to any change to a higher security level.

5 Where a ship is not in compliance with the requirements of this chapter or of part A of the ISPS Code, or cannot comply with the requirements of the security level set by the Administration or by another Contracting Government and applicable to that ship, then the ship shall notify the appropriate competent authority prior to conducting any ship/port interface or prior to entry into port, whichever occurs earlier.

Regulation 5—Specific Responsibility of Companies

The Company shall ensure that the master has available on board, at all times, information through which officers duly authorised by a Contracting Government can establish:

.1 Who is responsible for appointing the members of the crew or other persons

currently employed or engaged on board the ship in any capacity on the business of that ship;

.2 Who is responsible for deciding the employment of the ship; and

.3 In cases where the ship is employed under the terms of charter party(ies), who are the parties to such charter party(ies).

Regulation 6—Ship Security Alert System

1 All ships shall be provided with a ship security alert system, as follows:

.1 Ships constructed on or after July 1, 2004;

.2 Passenger ships, including high-speed passenger craft, constructed before July 1, 2004, not later than the first survey of the radio installation after July 1, 2004;

.3 Oil tankers, chemical tankers, gas carriers, bulk carriers and cargo high speed craft, of 500 gross tonnage and upwards constructed before July 1, 2004, not later than the first survey of the radio installation after July 1, 2004; and

.4 Other cargo ships of 500 gross tonnage and upward and mobile offshore drilling units constructed before July 1, 2004, not later than the first survey of the radio installation after July 1, 2006.

2 The ship security alert system, when activated, shall:

.1 Initiate and transmit a ship-to-shore security alert to a competent authority designated by the Administration, which in these circumstances may include the Company, identifying the ship, its location and indicating that the security of the ship is under threat or it has been compromised;

.2 Not send the ship security alert to any other ships;

.3 Not raise any alarm on-board the ship; and

.4 Continue the ship security alert until deactivated and/or reset.

3 The ship security alert system shall:

.1 Be capable of being activated from the navigation bridge and in at least one other location; and

.2 Conform to performance standards not inferior to those adopted by the Organization.

4 The ship security alert system activation points shall be designed so as to prevent the inadvertent initiation of the ship security alert.

5 The requirement for a ship security alert system may be complied with by using the radio installation fitted for compliance with the requirements of chapter IV, provided all requirements of this regulation are complied with.

6 When an Administration receives notification of a ship security alert, that Administration shall immediately notify the State(s) in the vicinity of which the ship is presently operating.

7 When a Contracting Government receives notification of a ship security alert from a ship which is not entitled to fly its flag, that Contracting Government shall immediately notify the relevant Administration and, if appropriate, the State(s) in the vicinity of which the ship is presently operating.

Regulation 7—Threats to Ships

1 Contracting Governments shall set security levels and ensure the provision of

security level information to ships operating in their territorial sea or having communicated an intention to enter their territorial sea.

2 Contracting Governments shall provide a point of contact through which such ships can request advice or assistance and to which such ships can report any security concerns about other ships, movements or communications.

3 Where a risk of attack has been identified, the Contracting Government concerned shall advise the ships concerned and their Administrations of:

.1 The current security level;

.2 Any security measures that should be put in place by the ships concerned to protect themselves from attack, in accordance with the provisions of part A of the ISPS Code; and

.3 Security measures that the coastal State has decided to put in place, as appropriate.

Regulation 8—Master's Discretion for Ship Safety and Security

1 The master shall not be constrained by the Company, the charterer or any other person from taking or executing any decision which, in the professional judgement of the master, is necessary to maintain the safety and security of the ship. This includes denial of access to persons (except those identified as duly authorized by a Contracting Government) or their effects and refusal to load cargo, including containers or other closed cargo transport units.

2 If, in the professional judgement of the master, a conflict between any safety and security requirements applicable to the ship arises during its operations, the master shall give effect to those requirements necessary to maintain the safety of the ship. In such cases, the master may implement temporary security measures and shall forthwith inform the Administration and, if appropriate, the Contracting Government in whose port the ship is operating or intends to enter. Any such temporary security measures under this regulation shall, to the highest possible degree, be commensurate with the prevailing security level. When such cases are identified, the Administration shall ensure that such conflicts are resolved and that the possibility of recurrence is minimised.

Regulation 9—Control and Compliance Measures

1 Control of Ships in Port.

1.1 For the purpose of this chapter, every ship to which this chapter applies is subject to control when in a port of another Contracting Government by officers duly authorised by that Government, who may be the same as those carrying out the functions of regulation I/19. Such control shall be limited to verifying that there is onboard a valid International Ship Security Certificate or a valid Interim International Ships Security Certificate issued under the provisions of part A of the ISPS Code (Certificate), which if valid shall be accepted, unless there are clear grounds for believing that the ship is not in compliance with the requirements of this chapter or part A of the ISPS Code.

1.2 When there are such clear grounds, or where no valid Certificate is produced when

required, the officers duly authorized by the Contracting Government shall impose any one or more control measures in relation to that ship as provided in paragraph 1.3. Any such measures imposed must be proportionate, taking into account the guidance given in part B of the ISPS Code.

1.3 Such control measures are as follows: inspection of the ship, delaying the ship, detention of the ship, restriction of operations including movement within the port, or expulsion of the ship from port. Such control measures may additionally or alternatively include other lesser administrative or corrective measures.

2 Ships Intending To Enter a Port of Another Contracting Government.

2.1 For the purpose of this chapter, a Contracting Government may require that ships intending to enter its ports provide the following information to officers duly authorized by that Government to ensure compliance with this chapter prior to entry into port with the aim of avoiding the need to impose control measures or steps:

.1 That the ship possesses a valid Certificate and the name of its issuing authority;

.2 The security level at which the ship is currently operating;

.3 The security level at which the ship operated in any previous port where it has conducted a ship/port interface within the timeframe specified in paragraph 2.3;

.4 Any special or additional security measures that were taken by the ship in any previous port where it has conducted a ship/port interface within the timeframe specified in paragraph 2.3;

.5 That the appropriate ship security procedures were maintained during any ship to ship activity within the timeframe specified in paragraph 2.3; or

.6 Other practical security related information (but not details of the ship security plan), taking into account the guidance given in part B of the ISPS Code.

If requested by the Contracting Government, the ship or the Company shall provide confirmation, acceptable to that Contracting Government, of the information required above.

2.2 Every ship to which this chapter applies intending to enter the port of another Contracting Government shall provide the information described in paragraph 2.1 on the request of the officers duly authorized by that Government. The master may decline to provide such information on the understanding that failure to do so may result in denial of entry into port.

2.3 The ship shall keep records of the information referred to in paragraph 2.1 for the last 10 calls at port facilities.

2.4 If, after receipt of the information described in paragraph 2.1, officers duly authorised by the Contracting Government of the port in which the ship intends to enter have clear grounds for believing that the ship is in non-compliance with the requirements of this chapter or part A of the ISPS Code, such officers shall attempt to establish communication with and between the ship and the Administration in order to rectify the non-compliance. If such communication does not result in rectification, or if such officers

have clear grounds otherwise for believing that the ship is in non-compliance with the requirements of this chapter or part A of the ISPS Code, such officers may take steps in relation to that ship as provided in paragraph 2.5. Any such steps taken must be proportionate, taking into account the guidance given in part B of the ISPS Code.

2.5 Such steps are as follows:

.1 A requirement for the rectification of the non-compliance;

.2 A requirement that the ship proceed to a location specified in the territorial sea or internal waters of that Contracting Government;

.3 Inspection of the ship, if the ship is in the territorial sea of the Contracting Government the port of which the ship intends to enter; or

.4 Denial of entry into port.

Prior to initiating any such steps, the ship shall be informed by the Contracting Government of its intentions. Upon this information the master may withdraw the intention to enter that port. In such cases, this regulation shall not apply.

3 Additional provisions.

3.1 In the event:

.1 Of the imposition of a control measure, other than a lesser administrative or corrective measure, referred to in paragraph 1.3; or

.2 Any of the steps referred to in paragraph 2.5 are taken,

An officer duly authorized by the Contracting Government shall forthwith inform in writing the Administration specifying which control measures have been imposed or steps taken and the reasons thereof. The Contracting Government imposing the control measures or steps shall also notify the recognized security organization which issued the Certificate relating to the ship concerned and the Organization when any such control measures have been imposed or steps taken.

3.2 When entry into port is denied or the ship is expelled from port, the authorities of the port State should communicate the appropriate facts to the authorities of the State of the next appropriate ports of call, when known, and any other appropriate coastal States, taking into account guidelines to be developed by the Organization. Confidentiality and security of such notification shall be ensured.

3.3 Denial of entry into port, pursuant to paragraphs 2.4 and 2.5, or expulsion from port, pursuant to paragraphs 1.1 to 1.3, shall only be imposed where the officers duly authorized by the Contracting Government have clear grounds to believe that the ship poses an immediate threat to the security or safety of persons, or of ships or other property and there are no other appropriate means for removing that threat.

3.4 The control measures referred to in paragraph 1.3 and the steps referred to in paragraph 2.5 shall only be imposed, pursuant to this regulation, until the non-compliance giving rise to the control measures or steps has been corrected to the satisfaction of the Contracting Government, taking into account actions proposed by the ship or the Administration, if any.

3.5 When Contracting Governments exercise control under paragraph 1 or take steps under paragraph 2:

.1 All possible efforts shall be made to avoid a ship being unduly detained or delayed. If a ship is thereby unduly detained, or delayed, it shall be entitled to compensation for any loss or damage suffered; and

.2 Necessary access to the ship shall not be prevented for emergency or humanitarian reasons and for security purposes.

Regulation 10—Requirements for Port Facilities

1 Port facilities shall comply with the relevant requirements of this chapter and part A of the ISPS Code, taking into account the guidance given in part B of the ISPS Code.

2 Contracting Governments with a port facility or port facilities within their territory, to which this regulation applies, shall ensure that:

.1 Port facility security assessments are carried out, reviewed and approved in accordance with the provisions of part A of the ISPS Code; and

.2 Port facility security plans are developed, reviewed, approved and implemented in accordance with the provisions of part A of the ISPS Code.

3 Contracting Governments shall designate and communicate the measures required to be addressed in a port facility security plan for the various security levels, including when the submission of a Declaration of Security will be required.

Regulation 11—Alternative Security Agreements

1 Contracting Governments may, when implementing this chapter and part A of the ISPS Code, conclude in writing bilateral or multilateral agreements with other Contracting Governments on alternative security arrangements covering short international voyages on fixed routes between port facilities located within their territories.

2 Any such agreement shall not compromise the level of security of other ships or of port facilities not covered by the agreement.

3 No ship covered by such an agreement shall conduct any ship-to-ship activities with any ship not covered by the agreement.

4 Such agreements shall be reviewed periodically, taking into account the experience gained as well as any changes in the particular circumstances or the assessed threats to the security of the ships, the port facilities or the routes covered by the agreement.

Regulation 12—Equivalent Security Arrangements

1 An Administration may allow a particular ship or a group of ships entitled to fly its flag to implement other security measures equivalent to those prescribed in this chapter or in part A of the ISPS Code, provided such security measures are at least as effective as those prescribed in this chapter or part A of the ISPS Code. The Administration, which allows such security measures, shall communicate to the Organization particulars thereof.

2 When implementing this chapter and part A of the ISPS Code, a Contracting

Government may allow a particular port facility or a group of port facilities located within its territory, other than those covered by an agreement concluded under regulation 11, to implement security measures equivalent to those prescribed in this chapter or in part A of the ISPS Code, provided such security measures are at least as effective as those prescribed in this chapter or part A of the ISPS Code. The Contracting Government, which allows such security measures, shall communicate to the Organization particulars thereof.

Regulation 13—Communication of Information

1 Contracting Governments shall, not later than July 1, 2004, communicate to the Organization and shall make available for the information of Companies and ships:

.1 The names and contact details of their national authority or authorities responsible for ship and port facility security;

.2 The locations within their territory covered by the approved port facility security plans.

.3 The names and contact details of those who have been designated to be available at all times to receive and act upon the ship-to-shore security alerts, referred to in regulation 6.2.1;

.4 The names and contact details of those who have been designated to be available at all times to receive and act upon any communications from Contracting Governments exercising control and compliance measures, referred to in regulation 9.3.1; and

.5 The names and contact details of those who have been designated to be available at all times to provide advice or assistance to ships and to whom ships can report any security concerns, referred to in regulation 7.2;

And thereafter update such information as and when changes relating thereto occur. The Organisation shall circulate such particulars to other Contracting Governments for the information of their officers.

2 Contracting Governments shall, not later than July 1, 2004, communicate to the Organization the names and contact details of any recognized security organizations authorized to act on their behalf together with details of the specific responsibility and conditions of authority delegated to such organizations. Such information shall be updated as and when changes relating thereto occur. The Organisation shall circulate such particulars to other Contracting Governments for the information of their officers.

3 Contracting Governments shall, not later than July 1, 2004 communicate to the Organization a list showing the approved port facility security plans for the port facilities located within their territory together with the location or locations covered by each approved port facility security plan and the corresponding date of approval and thereafter shall further communicate when any of the following changes take place:

.1 Changes in the location or locations covered by an approved port facility security plan are to be introduced or have been

introduced. In such cases the information to be communicated shall indicate the changes in the location or locations covered by the plan and the date as of which such changes are to be introduced or were implemented;

.2 An approved port facility security plan, previously included in the list submitted to the Organization, is to be withdrawn or has been withdrawn. In such cases, the information to be communicated shall indicate the date on which the withdrawal will take effect or was implemented. In these cases, the communication shall be made to the Organization as soon as is practically possible; and

.3 Additions are to be made to the list of approved port facility security plans. In such cases, the information to be communicated shall indicate the location or locations covered by the plan and the date of approval.

4 Contracting Governments shall, at five year intervals after July 1, 2004, communicate to the Organization a revised and updated list showing all the approved port facility security plans for the port facilities located within their territory together with the location or locations covered by each approved port facility security plan and the corresponding date of approval (and the date of approval of any amendments thereto) which will supersede and replace all information communicated to the Organization, pursuant to paragraph 3, during the preceding five years.

5 Contracting Governments shall communicate to the Organization information that an agreement under regulation 11 has been concluded. The information communicated shall include:

.1 The names of the Contracting Governments which have concluded the agreement;

.2 The port facilities and the fixed routes covered by the agreement;

.3 The periodicity of review of the agreement;

.4 The date of entry into force of the agreement; and

.5 Information on any consultations which have taken place with other Contracting Governments;

And thereafter shall communicate, as soon as practically possible, to the Organization information when the agreement has been amended or has ended.

6 Any Contracting Government which allows, under the provisions of regulation 12, any equivalent security arrangements with respect to a ship entitled to fly its flag or with respect to a port facility located within its territory, shall communicate to the Organization particulars thereof.

7 The Organization shall make available the information communicated under paragraph 3 to other Contracting Governments upon request.

International Code for the Security of Ships and of Port Facilities

Preamble

1 The Diplomatic Conference on Maritime Security held in London in December 2002 adopted new provisions in the International Convention for the Safety of Life at Sea, 1974 and this Code to enhance

maritime security. These new requirements form the international framework through which ships and port facilities can co-operate to detect and deter acts which threaten security in the maritime transport sector.

2 Following the tragic events of September 11, 2001, the twenty-second session of the Assembly of the International Maritime Organization (the Organization), in November 2001, unanimously agreed to the development of new measures relating to the security of ships and of port facilities for adoption by a Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 (known as the Diplomatic Conference on Maritime Security) in December 2002. Preparation for the Diplomatic Conference was entrusted to the Organization's Maritime Safety Committee (MSC) on the basis of submissions made by Member States, intergovernmental organizations and non-governmental organizations in consultative status with the Organization.

3 The MSC, at its first extraordinary session, held also in November 2001, in order to accelerate the development and the adoption of the appropriate security measures established an MSC Intersessional Working Group on Maritime Security. The first meeting of the MSC Intersessional Working Group on Maritime Security was held in February 2002 and the outcome of its discussions was reported to, and considered by, the seventy-fifth session of the MSC in March 2002, when an ad hoc Working Group was established to further develop the proposals made. The seventy-fifth session of the MSC considered the report of that Working Group and recommended that work should be taken forward through a further MSC Intersessional Working Group, which was held in September 2002. The seventy-sixth session of the MSC considered the outcome of the September 2002 session of the MSC Intersessional Working Group and the further work undertaken by the MSC Working Group held in conjunction with the Committee's seventy-sixth session in December 2002, immediately prior to the Diplomatic Conference and agreed the final version of the proposed texts to be considered by the Diplomatic Conference.

4 The Diplomatic Conference (December 9 to 13, 2002) also adopted amendments to the existing provisions of the International Convention for the Safety of Life at Sea, 1974 (SOLAS 74) accelerating the implementation of the requirement to fit Automatic Identification Systems and adopted new regulations in chapter XI-1 of SOLAS 74 covering marking of the Ship's Identification Number and the carriage of a Continuous Synopsis Record. The Diplomatic Conference also adopted a number of Conference Resolutions including those covering implementation and revision of this Code, Technical Co-operation, and co-operative work with the International Labour Organization and World Customs Organization. It was recognised that review and amendment of certain of the new provisions regarding maritime security may be required on completion of the work of these two Organizations.

5 The provision of chapter XI-2 of SOLAS 74 and this Code apply to ships and

to port facilities. The extension of SOLAS 74 to cover port facilities was agreed on the basis that SOLAS 74 offered the speediest means of ensuring the necessary security measures entered into force and given effect quickly. However, it was further agreed that the provisions relating to port facilities should relate solely to the ship/port interface. The wider issue of the security of port areas will be the subject of further joint work between the International Maritime Organization and the International Labour Organization. It was also agreed that the provisions should not extend to the actual response to attacks or to any necessary clear-up activities after such an attack.

6 In drafting the provision care has been taken to ensure compatibility with the provisions of the International Convention on Standards of Training, Certification and Watch-keeping and Certification for Seafarers, 1978, as amended, the International Safety Management (ISM) Code and the harmonised system of survey and certification.

7 The provisions represent a significant change in the approach of the international maritime industries to the issue of security in the maritime transport sector. It is recognised that they may place a significant additional burden on certain Contracting Governments. The importance of Technical Co-operation to assist Contracting Governments implement the provisions is fully recognised.

8 Implementation of the provisions will require continuing effective co-operation and understanding between all those involved with, or using, ships and port facilities including ship's personnel, port personnel, passengers, cargo interests, ship and port management and those in National and Local Authorities with security responsibilities. Existing practices and procedures will have to be reviewed and changed if they do not provide an adequate level of security. In the interests of enhanced maritime security additional responsibilities will have to be carried by the shipping and port industries and by National and Local Authorities.

9 The guidance given in part B of this Code should be taken into account when implementing the security provisions set out in chapter XI-2 of SOLAS 74 and in part A of this Code. However, it is recognised that the extent to which the guidance applies may vary depending on the nature of the port facility and of the ship, its trade and/or cargo.

10 Nothing in this Code shall be interpreted or applied in a manner inconsistent with the proper respect of fundamental rights and freedoms as set out in international instruments, particularly those relating to maritime workers and refugees including the International Labour Organisation Declaration of Fundamental Principles and Rights at Work as well as international standards concerning maritime and port workers.

11 Recognizing that the Convention on the Facilitation of Maritime Traffic, 1965, as amended, provides that foreign crew members shall be allowed ashore by the public authorities while the ship on which they arrive is in port, provided that the formalities on arrival of the ship have been fulfilled and the public authorities have no

reason to refuse permission to come ashore for reasons of public health, public safety or public order, Contracting Governments when approving ship and port facility security plans should pay due cognisance to the fact that ship's personnel live and work on the vessel and need shore leave and access to shore based seafarer welfare facilities, including medical care.

Part A—The Safety of Life at Sea, 1974 as Amended

Mandatory Requirements Regarding the Provisions of Chapter XI-2 of the International Convention for the Safety of Life At Sea, 1974, As Amended

1 General

1.1 Introduction.

This part of the International Code for the Security of Ships and Port Facilities contains mandatory provisions to which reference is made in chapter XI-2 of the International Convention for the Safety of Life at Sea, 1974 as amended.

1.2 Objectives.

The objectives of this Code are:

.1 To establish an international framework involving co-operation between Contracting Governments, Government agencies, local administrations and the shipping and port industries to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade;

.2 To establish the respective roles and responsibilities of the Contracting Governments, Government agencies, local administrations and the shipping and port industries, at the national and international level for ensuring maritime security;

.3 To ensure the early and efficient collection and exchange of security-related information;

.4 To provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels; and

.5 To ensure confidence that adequate and proportionate maritime security measures are in place.

1.3 Functional requirements.

In order to achieve its objectives, this Code embodies a number of functional requirements. These include, but are not limited to:

.1 Gathering and assessing information with respect to security threats and exchanging such information with appropriate Contracting Governments;

.2 Requiring the maintenance of communication protocols for ships and port facilities;

.3 Preventing unauthorized access to ships, port facilities and their restricted areas;

.4 Preventing the introduction of unauthorized weapons, incendiary devices or explosives to ships or port facilities;

.5 Providing means for raising the alarm in reaction to security threats or security incidents;

.6 Requiring ship and port facility security plans based upon security assessments; and

.7 Requiring training, drills and exercises to ensure familiarity with security plans and procedures.

2 Definitions

2.1 For the purpose of this part, unless expressly provided otherwise:

.1 Convention means the International Convention for the Safety of Life at Sea, 1974 as amended.

.2 Regulation means a regulation of the Convention.

.3 Chapter means a chapter of the Convention.

.4 Ship security plan means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident.

.5 Port facility security plan means a plan developed to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident.

.6 Ship security officer means the person on board the ship, accountable to the master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the ship security plan and for liaison with the company security officer and port facility security officers.

.7 Company security officer means the person designated by the Company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval, and thereafter implemented and maintained and for liaison with port facility security officers and the ship security officer.

.8 Port facility security officer means the person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers.

.9 Security level 1 means the level for which minimum appropriate protective security measures shall be maintained at all times.

.10 Security level 2 means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

.11 Security level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

2.2 The term "ship", when used in this Code, includes mobile offshore drilling units and high-speed craft as defined in regulation XI-2/1.

2.3 The term "Contracting Government" in connection with any reference to a port facility, when used in sections 14 to 18, includes a reference to the "Designated Authority".

2.4 Terms not otherwise defined in this part shall have the same meaning as the meaning attributed to them in chapters I and XI-2.

3 Application

3.1 This Code applies to:

- .1 The following types of ships engaged on international voyages:
 - .1 Passenger ships, including high-speed passenger craft;
 - .2 Cargo ships, including high-speed craft, of 500 gross tonnage and upwards; and
 - .3 Mobile offshore drilling units; and
 - .2 Port facilities serving such ships engaged on international voyages.

3.2 Notwithstanding the provisions of section 3.1.2, Contracting Governments shall decide the extent of application of this part of the Code to those port facilities within their territory which, although used primarily by ships not engaged on international voyages, are required, occasionally, to serve ships arriving or departing on an international voyage.

3.2.1 Contracting Governments shall base their decisions, under section 3.2, on a port facility security assessment carried out in accordance with this part of the Code.

3.2.2 Any decision which a Contracting Government makes, under section 3.2, shall not compromise the level of security intended to be achieved by chapter XI-2 or by this part of the Code.

3.3 This Code does not apply to warships, naval auxiliaries or other ships owned or operated by a Contracting Government and used only on Government non-commercial service.

3.4 Sections 5 to 13 and 19 of this part apply to Companies and ships as specified in regulation XI-2/4.

3.5 Sections 5 and 14 to 18 of this part apply to port facilities as specified in regulation XI-2/10.

3.6 Nothing in this Code shall prejudice the rights or obligations of States under international law.

4 Responsibilities of Contracting Governments

4.1 Subject to the provisions of regulation XI-2/3 and XI-2/7, Contracting Governments shall set security levels and provide guidance for protection from security incidents. Higher security levels indicate greater likelihood of occurrence of a security incident. Factors to be considered in setting the appropriate security level include:

- .1 The degree that the threat information is credible;
- .2 The degree that the threat information is corroborated;
- .3 The degree that the threat information is specific or imminent; and
- .4 The potential consequences of such a security incident.

4.2 Contracting Governments, when they set security level 3, shall issue, as necessary, appropriate instructions and shall provide security related information to the ships and port facilities that may be affected.

4.3 Contracting Governments may delegate to a recognized security organization certain of their security related duties under chapter XI-2 and this part of the Code with the exception of:

- .1 Setting of the applicable security level;
- .2 Approving a Port Facility Security Assessment and subsequent amendments to an approved assessment;

.3 Determining the port facilities which will be required to designate a Port Facility Security Officer;

.4 Approving a Port Facility Security Plan and subsequent amendments to an approved plan;

.5 Exercising control and compliance measures pursuant to regulation XI-2/9; and

.6 Establishing the requirements for a Declaration of Security.

4.4 Contracting Governments shall, to the extent they consider appropriate, test the effectiveness of the Ship or the Port Facility Security Plans, or of amendments to such plans, they have approved, or, in the case of ships, of plans which have been approved on their behalf.

5 Declaration of Security

5.1 Contracting Governments shall determine when a Declaration of Security is required by assessing the risk the ship/port interface or ship to ship activity poses to people, property or the environment.

5.2 A ship can request completion of a Declaration of Security when:

- .1 The ship is operating at a higher security level than the port facility or another ship it is interfacing with;
- .2 There is an agreement on Declarations of Security between Contracting Governments covering certain international voyages or specific ships on those voyages;
- .3 There has been a security threat or a security incident involving the ship or involving the port facility, as applicable;
- .4 The ship is at a port which is not required to have and implement an approved port facility security plan; or
- .5 The ship is conducting ship to ship activities with another ship not required to have and implement an approved ship security plan.

5.3 Requests for the completion of a Declaration of Security, under this section, shall be acknowledged by the applicable port facility or ship.

5.4 The Declaration of Security shall be completed by:

- .1 The master or the ship security officer on behalf of the ship(s); and, if appropriate,
- .2 The port facility security officer or, if the Contracting Government determines otherwise, by any other body responsible for shore-side security, on behalf of the port facility.

5.5 The Declaration of Security shall address the security requirements that could be shared between a port facility and a ship (or between ships) and shall state the responsibility for each.

5.6 Contracting Governments shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by the port facilities located within their territory.

5.7 Administrations shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by ships entitled to fly their flag.

6 Obligations of the Company

6.1 The Company shall ensure that the ship security plan contains a clear statement emphasizing the master's authority. The

Company shall establish in the ship security plan that the master has the overriding authority and responsibility to make decisions with respect to the security of the ship and to request the assistance of the Company or of any Contracting Government as may be necessary.

6.2 The Company shall ensure that the company security officer, the master and the ship security officer are given the necessary support to fulfil their duties and responsibilities in accordance with chapter XI-2 and this part of the Code.

7 Ship Security

7.1 A ship is required to act upon the security levels set by Contracting Governments as set out below.

7.2 At security level 1, the following activities shall be carried out, through appropriate measures, on all ships, taking into account the guidance given in part B of this Code, in order to identify and take preventive measures against security incidents:

- .1 Ensuring the performance of all ship security duties;
- .2 Controlling access to the ship;
- .3 Controlling the embarkation of persons and their effects;
- .4 Monitoring restricted areas to ensure that only authorized persons have access;
- .5 Monitoring of deck areas and areas surrounding the ship;
- .6 Supervising the handling of cargo and ship's stores; and
- .7 Ensuring that security communication is readily available.

7.3 At security level 2, the additional protective measures, specified in the ship security plan, shall be implemented for each activity detailed in section 7.2, taking into account the guidance given in part B of this Code.

7.4 At security level 3, further specific protective measures, specified in the ship security plan, shall be implemented for each activity detailed in section 7.2, taking into account the guidance given in part B of this Code.

7.5 Whenever security level 2 or 3 is set by the Administration, the ship shall acknowledge receipt of the instructions on change of the security level.

7.6 Prior to entering a port, or whilst in a port within the territory of a Contracting Government that has set security level 2 or 3, the ship shall acknowledge receipt of this instruction and shall confirm to the port facility security officer the initiation of the implementation of the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3 in instructions issued by the Contracting Government which has set security level 3. The ship shall report any difficulties in implementation. In such cases, the port facility security officer and ship security officer shall liaise and co-ordinate the appropriate actions.

7.7 If a ship is required by the Administration to set, or is already at, a higher security level than that set for the port it intends to enter or in which it is already located, then the ship shall advise, without delay, the competent authority of the Contracting Government within whose

territory the port facility is located and the port facility security officer of the situation.

7.7.1 In such cases, the ship security officer shall liaise with the port facility security officer and co-ordinate appropriate actions, if necessary.

7.8 An Administration requiring ships entitled to fly its flag to set security level 2 or 3 in a port of another Contracting Government shall inform that Contracting Government without delay.

7.9 When Contracting Governments set security levels and ensure the provision of security level information to ships operating in their territorial sea, or having communicated an intention to enter their territorial sea, such ships shall be advised to maintain vigilance and report immediately to their Administration and any nearby coastal States any information that comes to their attention that might affect maritime security in the area.

7.9.1 When advising such ships of the applicable security level, a Contracting Government shall, taking into account the guidance given in the part B of this Code, also advise those ships of any security measure that they should take and, if appropriate, of measures that have been taken by the Contracting Government to provide protection against the threat.

8 Ship Security Assessment

8.1 The ship security assessment is an essential and integral part of the process of developing and updating the ship security plan.

8.2 The company security officer shall ensure that the ship security assessment is carried out by persons with appropriate skills to evaluate the security of a ship, in accordance with this section, taking into account the guidance given in part B of this Code.

8.3 Subject to the provisions of section 9.2.1, a recognised security organisation may carry out the ship security assessment of a specific ship.

8.4 The ship security assessment shall include an on-scene security survey and, at least, the following elements:

- .1 Identification of existing security measures, procedures and operations;
- .2 Identification and evaluation of key ship board operations that it is important to protect;
- .3 Identification of possible threats to the key ship board operations and the likelihood of their occurrence, in order to establish and prioritise security measures; and
- .4 Identification of weaknesses, including human factors in the infrastructure, policies and procedures.

8.5 The ship security assessment shall be documented, reviewed, accepted and retained by the Company.

9 Ship Security Plan

9.1 Each ship shall carry on board a ship security plan approved by the Administration. The plan shall make provisions for the three security levels as defined in this part of the Code.

9.1.1 Subject to the provisions of section 9.2.1, a recognised security organisation may prepare the ship security plan for a specific ship.

9.2 The Administration may entrust the review and approval of ship security plans, or of amendments to a previously approved plan, to recognised security organisations.

9.2.1 In such cases the recognised security organisation, undertaking the review and approval of a ship security plan, or its amendments, for a specific ship shall not have been involved in either the preparation of the ship security assessment or of the ship security plan, or of the amendments, under review.

9.3 The submission of a ship security plan, or of amendments to a previously approved plan, for approval shall be accompanied by the security assessment on the basis of which the plan, or the amendments, have been developed.

9.4 Such a plan shall be developed, taking into account the guidance given in part B of this Code and shall be written in the working language or languages of the ship. If the language or languages used is not English, French or Spanish, a translation into one of these languages shall be included. The plan shall address, at least, the following:

- .1 Measures designed to prevent weapons, dangerous substances and devices intended for use against people, ships or ports and the carriage of which is not authorized from being taken on board the ship;
- .2 Identification of the restricted areas and measures for the prevention of unauthorized access to them;
- .3 Measures for the prevention of unauthorized access to the ship;
- .4 Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;
- .5 Procedures for responding to any security instructions Contracting Governments may give at security level 3;
- .6 Procedures for evacuation in case of security threats or breaches of security;
- .7 Duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;
- .8 Procedures for auditing the security activities;
- .9 Procedures for training, drills and exercises associated with the plan;
- .10 Procedures for interfacing with port facility security activities;
- .11 Procedures for the periodic review of the plan and for updating;
- .12 Procedures for reporting security incidents;
- .13 Identification of the ship security officer;
- .14 Identification of the company security officer including with 24-hour contact details;
- .15 Procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board, if any;
- .16 Frequency for testing or calibration any security equipment provided on board, if any;
- .17 Identification of the locations where the ship security alert system activation points are provided;¹ and

¹ Administrations may allow, in order to avoid any compromising of the objective of providing on

.18 Procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.¹

9.4.1 Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the Company or of the ship.

9.5 The Administration shall determine which changes to an approved ship security plan or to any security equipment specified in an approved plan shall not be implemented unless the relevant amendments to the plan are approved by the Administration. Any such changes shall be at least as effective as those measures prescribed in chapter XI-2 and this part of the Code.

9.5.1 The nature of the changes to the ship security plan or the security equipment that have been specifically approved by the Administration, pursuant to section 9.5, shall be documented in a manner that clearly indicates such approval. This approval shall be available on board and shall be presented together with the International Ship Security Certificate (or the Interim International Ship Security Certificate). If these changes are temporary, once the original approved measures or equipment are reinstated, this documentation no longer needs to be retained by the ship.

9.6 The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorised deletion, destruction or amendment.

9.7 The plan shall be protected from unauthorized access or disclosure.

9.9 Ship security plans are not subject to inspection by officers duly authorised by a Contracting Government to carry out control and compliance measures in accordance with regulation XI-2/9, save in circumstances specified in section 9.9.1.

9.9.1 If the officers duly authorised by a Contracting Government have clear grounds to believe that the ship is not in compliance with the requirements of chapter XI-2 or part A of this Code, and the only means to verify or rectify the non-compliance is to review the relevant requirements of the ship security plan, limited access to the specific sections of the plan relating to the non-compliance is exceptionally allowed, but only with the consent of the Contracting Government of, or the master of, the ship concerned. Nevertheless, the provisions in the plan relating to section 9.4 subsections .2, .4, .5, .7, .15, .17 and .18 of this part of the Code are considered as confidential information, and cannot be subject to inspection unless otherwise agreed by the Contracting Governments concerned.

10 Records

10.1 Records of the following activities addressed in the ship security plan shall be kept on board for at least the minimum

board the ship security alert system, this information to be kept elsewhere on board in a document known to the master, the ship security officer and other senior shipboard personnel as may be decided by the Company.

period specified by the Administration, bearing in mind the provisions of regulation XI-2/9.2.3:

- .1 Training, drills and exercises;
- .2 Security threats and security incidents;
- .3 Breaches of security;
- .4 Changes in security level;
- .5 Communications relating to the direct security of the ship such as specific threats to the ship or to port facilities the ship is, or has been;
- .6 Internal audits and reviews of security activities;
- .7 Periodic review of the ship security assessment;
- .8 Periodic review of the ship security plan;
- .9 Implementation of any amendments to the plan; and
- .10 Maintenance, calibration and testing of security equipment, if any including testing of the ship security alert system.

10.2 The records shall be kept in the working language or languages of the ship. If the language or languages used are not English, French or Spanish, a translation into one of these languages shall be included.

10.3 The records may be kept in an electronic format. In such a case, they shall be protected by procedures aimed at preventing their unauthorised deletion, destruction or amendment.

10.4 The records shall be protected from unauthorized access or disclosure.

11 Company Security Officer

11.1 The Company shall designate a company security officer. A person designated as the company security officer may act as the company security officer for one or more ships, depending on the number or types of ships the Company operates provided it is clearly identified for which ships this person is responsible. A Company may, depending on the number or types of ships they operate designate several persons as company security officers provided it is clearly identified for which ships each person is responsible.

11.2 In addition to those specified elsewhere in this part of the Code, the duties and responsibilities of the company security officer shall include, but are not limited to:

- .1 Advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information;
- .2 Ensuring that ship security assessments are carried out;
- .3 Ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan;
- .4 Ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship;
- .5 Arranging for internal audits and reviews of security activities;
- .6 Arranging for the initial and subsequent verifications of the ship by the Administration or the recognised security organisation;
- .7 Ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections

and verifications of compliance are promptly addressed and dealt with;

- .8 Enhancing security awareness and vigilance;
- .9 Ensuring adequate training for personnel responsible for the security of the ship;
- .10 Ensuring effective communication and co-operation between the ship security officer and the relevant port facility security officers;
- .11 Ensuring consistency between security requirements and safety requirement;
- .12 Ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately; and
- .13 Ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.

12 Ship Security Officer

12.1 A ship security officer shall be designated on each ship.

12.2 In addition to those specified elsewhere in this part of the Code, the duties and responsibilities of the ship security officer shall include, but are not limited to:

- .1 Undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;
- .2 Maintaining and supervising the implementation of the ship security plan, including any amendments to the plan;
- .3 Co-ordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant port facility security officers;
- .4 Proposing modifications to the ship security plan;
- .5 Reporting to the Company Security Officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions;
- .6 Enhancing security awareness and vigilance on board;
- .7 Ensuring that adequate training has been provided to shipboard personnel, as appropriate;
- .8 Reporting all security incidents;
- .9 Co-ordinating implementation of the ship security plan with the company security officer and the relevant port facility security officer; and
- .10 Ensuring that security equipment is properly operated, tested, calibrated and maintained, if any.

13 Training, Drills and Exercises on Ship Security

13.1 The company security officer and appropriate shore-based personnel shall have knowledge and have received training, taking into account the guidance given in part B of this Code.

13.2 The ship security officer shall have knowledge and have received training, taking into account the guidance given in part B of this Code.

13.3 Shipboard personnel having specific security duties and responsibilities shall understand their responsibilities for ship

security as described in the ship security plan and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the guidance given in Part B of this Code.

13.4 To ensure the effective implementation of the ship security plan, drills shall be carried out at appropriate intervals taking into account the ship type, ship personnel changes, port facilities to be visited and other relevant circumstances, taking into account guidance given in part B of this Code.

13.5 The company security officer shall ensure the effective coordination and implementation of ship security plans by participating in exercises at appropriate intervals, taking into account the guidance given in part B of this Code.

14 Port Facility Security

14.1 A port facility is required to act upon the security levels set by the Contracting Government within whose territory it is located. Security measures and procedures shall be applied at the port facility in such a manner as to cause a minimum of interference with, or delay to, passengers, ship, ship's personnel and visitors, goods and services.

14.2 At security level 1, the following activities shall be carried out through appropriate measures in all port facilities, taking into account the guidance given in part B of this Code, in order to identify and take preventive measures against security incidents:

- .1 Ensuring the performance of all port facility security duties;
- .2 Controlling access to the port facility;
- .3 Monitoring of the port facility, including anchoring and berthing area(s);
- .4 Monitoring restricted areas to ensure that only authorized persons have access;
- .5 Supervising the handling of cargo;
- .6 Supervising the handling of ship's stores; and
- .7 Ensuring that security communication is readily available.

14.3 At security level 2, the additional protective measures, specified in the port facility security plan, shall be implemented for each activity detailed in section 14.2, taking into account the guidance given in part B of this Code.

14.4 At security level 3, further specific protective measures, specified in the port facility security plan, shall be implemented for each activity detailed in section 14.2, taking into account the guidance given in part B of this Code.

14.4.1 In addition, at security level 3, port facilities are required to respond to and implement any security instructions given by the Contracting Government within whose territory the port facility is located.

14.5 When a port facility security officer is advised that a ship encounters difficulties in complying with the requirements of chapter XI-2 or this part or in implementing the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3 following any security instructions given by the Contracting Government within whose territory the port facility is located, the port facility security

officer and ship security officer shall liaise and co-ordinate appropriate actions.

14.6 When a port facility security officer is advised that a ship is at a security level, which is higher than that of the port facility, shall report the matter to the competent authority and shall liaise with the ship security officer and co-ordinate appropriate actions, if necessary.

15 Port Facility Security Assessment

15.1 The port facility security assessment is an essential and integral part of the process of developing and updating the port facility security plan.

15.2 The port facility security assessment shall be carried out by the Contracting Government within whose territory the port facility is located. A Contracting Government may authorise a recognised security organisation to carry out the port facility security assessment of a specific port facility located within its territory.

15.2.1 When the port facility security assessment has been carried out by a recognised security organisation, the security assessment shall be reviewed and approved for compliance with this section by the Contracting Government within whose territory the port facility is located.

15.3 The persons carrying out the assessment shall have appropriate skills to evaluate the security of the port facility in accordance with this section, taking into account the guidance given in part B of this Code.

15.4 The port facility security assessments shall periodically be reviewed and updated, taking account of changing threats and/or minor changes in the port facility and shall always be reviewed and updated when major changes to the port facility take place.

15.5 The port facility security assessment shall include, at least, the following elements:

.1 Identification and evaluation of important assets and infrastructure it is important to protect;

.2 Identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures;

.3 Identification, selection and prioritization of counter measures and procedural changes and their level of effectiveness in reducing vulnerability; and

.4 Identification of weaknesses, including human factors in the infrastructure, policies and procedures.

15.6 The Contracting Government may allow a port facility security assessment to cover more than one port facility if the operator, location, operation, equipment, and design of these port facilities are similar. Any Contracting Government, which allows such an arrangement shall communicate to the Organization particulars thereof.

15.7 Upon completion of the port facility security assessment, a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment and a description of counter measures that could be used to address each vulnerability. The report shall be protected from unauthorized access or disclosure.

16 Port Facility Security Plan

16.1 A port facility security plan shall be developed and maintained, on the basis of a port facility security assessment, for each port facility, adequate for the ship/port interface. The plan shall make provisions for the three security levels, as defined in this part of the Code.

16.1.1 Subject to the provisions of section 16.2, a recognized security organization may prepare the port facility security plan of a specific port facility.

16.2 The port facility security plan shall be approved by the Contracting Government in whose territory the port facility is located.

16.3 Such a plan shall be developed taking into account the guidance given in part B of this Code and shall be in the working language of the port facility. The plan shall address, at least, the following:

.1 Measures designed to prevent weapons or any other dangerous substances and devices intended for use against people, ships or ports and the carriage of which is not authorized, from being introduced into the port facility or on board a ship;

.2 Measures designed to prevent unauthorized access to the port facility, to ships moored at the facility, and to restricted areas of the facility;

.3 Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port facility or ship/port interface;

.4 Procedures for responding to any security instructions the Contracting Government, in whose territory the port facility is located, may give at security level 3;

.5 Procedures for evacuation in case of security threats or breaches of security;

.6 Duties of port facility personnel assigned security responsibilities and of other facility personnel on security aspects;

.7 Procedures for interfacing with ship security activities;

.8 Procedures for the periodic review of the plan and updating;

.9 Procedures for reporting security incidents;

.10 Identification of the port facility security officer including 24-hour contact details;

.11 Measures to ensure the security of the information contained in the plan;

.12 Measures designed to ensure effective security of cargo and the cargo handling equipment at the port facility;

.13 Procedures for auditing the port facility security plan;

.14 Procedures for responding in case the ship security alert system of a ship at the port facility has been activated; and

.15 Procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship including representatives of seafarers' welfare and labour organizations.

16.3.1 Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the port facility.

16.4 The port facility security plan may be combined with, or be part of, the port

security plan or any other port emergency plan or plans.

16.5 The Contracting Government in whose territory the port facility is located shall determine which changes to the port facility security plan shall not be implemented unless the relevant amendments to the plan are approved by them.

16.6 The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorised deletion, destruction or amendment.

16.7 The plan shall be protected from unauthorized access or disclosure.

16.8 Contracting Governments may allow a port facility security plan to cover more than one port facility if the operator, location, operation, equipment, and design of these port facilities are similar. Any Contracting Government, which allows such an alternative arrangement, shall communicate to the Organization particulars thereof.

17 Port Facility Security Officer

17.1 A port facility security officer shall be designated for each port facility. A person may be designated as the port facility security officer for one or more port facilities.

17.2 In addition to those specified elsewhere in this part of the Code, the duties and responsibilities of the port facility security officer shall include, but are not limited to:

.1 Conducting an initial comprehensive security survey of the port facility taking into account the relevant port facility security assessment;

.2 Ensuring the development and maintenance of the port facility security plan;

.3 Implementing and exercising the port facility security plan;

.4 Undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures;

.5 Recommending and incorporating, as appropriate, modifications to the port facility security plan in order to correct deficiencies and to update the plan to take into account of relevant changes to the port facility;

.6 Enhancing security awareness and vigilance of the port facility personnel;

.7 Ensuring adequate training has been provided to personnel responsible for the security of the port facility;

.8 Reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility;

.9 Co-ordinating implementation of the port facility security plan with the appropriate Company and ship security officer(s);

.10 Co-ordinating with security services, as appropriate;

.11 Ensuring that standards for personnel responsible for security of the port facility are met;

.12 Ensuring that security equipment is properly operated, tested, calibrated and maintained, if any; and

.13 Assisting ship security officers in confirming the identity of those seeking to board the ship when requested.

17.3 The port facility security officer shall be given the necessary support to fulfil the duties and responsibilities imposed by chapter XI-2 and this part of this Code.

18 Training, Drills and Exercises on Port Facility Security

18.1 The port facility security officer and appropriate port facility security personnel shall have knowledge and have received training, taking into account the guidance given in part B of this Code.

18.2 Port facility personnel having specific security duties shall understand their duties and responsibilities for port facility security, as described in the port facility security plan and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the guidance given in part B of this Code.

18.3 To ensure the effective implementation of the port facility security plan, drills shall be carried out at appropriate intervals taking into account the types of operations of the port facility, port facility personnel changes, the type of ship the port facility is serving and other relevant circumstances, taking into account guidance given in part B of this Code.

18.4 The port facility security officer shall ensure the effective coordination and implementation of the port facility security plan by participating in exercises at appropriate intervals, taking into account the guidance given in part B of this Code.

19 Verification and Certification for Ships

19.1 Verifications.

19.1.1 Each ship to which this part of the Code applies shall be subject to the verifications specified below:

.1 An initial verification before the ship is put in service or before the certificate required under section 19.2 is issued for the first time, which shall include a complete verification of its security system and any associated security equipment covered by the relevant provisions of chapter XI-2, this part of the Code and the approved ship security plan. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of chapter XI-2 and this part of the Code, is in satisfactory condition and fit for the service for which the ship is intended;

.2 A renewal verification at intervals specified by the Administration, but not exceeding five years, except where section 19.3.1 or 19.3.4 is applicable. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of chapter XI-2, this part of the Code and the approved Ship Security Plan, is in satisfactory condition and fit for the service for which the ship is intended;

.3 At least one intermediate verification. If only one intermediate verification is carried out it shall take place between the second and third anniversary date of the certificate as defined in regulation I/2(n). The intermediate verification shall include inspection of the security system and any associated security equipment of the ship to ensure that it remains satisfactory for the

service for which the ship is intended. Such intermediate verification shall be endorsed on the certificate;

.4 Any additional verifications as determined by the Administration.

19.1.2 The verifications of ships shall be carried out by officers of the Administration. The Administration may, however, entrust the verifications to a recognized security organization referred to in regulation XI-2/1.

19.1.3 In every case, the Administration concerned shall fully guarantee the completeness and efficiency of the verification and shall undertake to ensure the necessary arrangements to satisfy this obligation.

19.1.4 The security system and any associated security equipment of the ship after verification shall be maintained to conform with the provisions of regulations XI-2/4.2 and XI-2/6, this part of the Code and the approved ship security plan. After any verification under section 19.1.1 has been completed, no changes shall be made in security system and in any associated security equipment or the approved ship security plan without the sanction of the Administration.

19.2 Issue or endorsement of certificate.

19.2.1 An International Ship Security Certificate shall be issued after the initial or renewal verification in accordance with the provisions of section 19.1.

19.2.2 Such certificate shall be issued or endorsed either by the Administration or by the a recognized security organization acting on behalf of the Administration.

19.2.3 Another Contracting Government may, at the request of the Administration, cause the ship to be verified and, if satisfied that the provisions of section 19.1.1 are complied with, shall issue or authorize the issue of an International Ship Security Certificate to the ship and, where appropriate, endorse or authorize the endorsement of that certificate on the ship, in accordance with this Code.

19.2.3.1 A copy of the certificate and a copy of the verification report shall be transmitted as soon as possible to the requesting Administration.

19.2.3.2 A certificate so issued shall contain a statement to the effect that it has been issued at the request of the Administration and it shall have the same force and receive the same recognition as the certificate issued under section 19.2.2.

19.2.4 The International Ship Security Certificate shall be drawn up in a form corresponding to the model given in the appendix to this Code. If the language used is not English, French or Spanish, the text shall include a translation into one of these languages.

19.3 Duration and validity of certificate.

19.3.1 An International Ship Security Certificate shall be issued for a period specified by the Administration which shall not exceed five years.

19.3.2 When the renewal verification is completed within three months before the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing certificate.

19.3.2.1 When the renewal verification is completed after the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing certificate.

19.3.2.2 When the renewal verification is completed more than three months before the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of completion of the renewal verification.

19.3.3 If a certificate is issued for a period of less than five years, the Administration may extend the validity of the certificate beyond the expiry date to the maximum period specified in section 19.3.1, provided that the verifications referred to in section 19.1.1 applicable when a certificate is issued for a period of five years are carried out as appropriate.

19.3.4 If a renewal verification has been completed and a new certificate cannot be issued or placed on board the ship before the expiry date of the existing certificate, the Administration or recognized security organization acting on behalf of the Administration may endorse the existing certificate and such a certificate shall be accepted as valid for a further period which shall not exceed five months from the expiry date.

19.3.5 If a ship at the time when a certificate expires is not in a port in which it is to be verified, the Administration may extend the period of validity of the certificate but this extension shall be granted only for the purpose of allowing the ship to complete its voyage to the port in which it is verified, and then only in cases where it appears proper and reasonable to do so. No certificate shall be extended for a period longer than three months, and the ship to which an extension is granted shall not, on its arrival in the port in which it is to be verified, be entitled by virtue of such extension to leave that port without having a new certificate. When the renewal verification is completed, the new certificate shall be valid to a date not exceeding five years from the expiry date of the existing certificate before the extension was granted.

19.3.6 A certificate issued to a ship engaged on short voyages which has not been extended under the foregoing provisions of this section may be extended by the Administration for a period of grace of up to one month from the date of expiry stated on it. When the renewal verification is completed, the new certificate shall be valid to a date not exceeding five years from the date of expiry of the existing certificate before the extension was granted.

19.3.7 If an intermediate verification is completed before the period specified in section 19.1.1, then:

.1 The expiry date shown on the certificate shall be amended by endorsement to a date which shall not be more than three years later than the date on which the intermediate verification was completed;

.2 The expiry date may remain unchanged provided one or more additional verifications are carried out so that the

maximum intervals between the verifications prescribed by section 19.1.1 are not exceeded.

19.3.8 A certificate issued under section 19.2 shall cease to be valid in any of the following cases:

- .1 If the relevant verifications are not completed within the periods specified under section 19.1.1;
- .2 If the certificate is not endorsed in accordance with section 19.1.1.3 and 19.3.7.2 if applicable;
- .3 When a Company assumes the responsibility for the operation of a ship not previously operated by that Company; and
- .4 Upon transfer of the ship to the flag of another State.

19.3.9 In the case of:

.1 A transfer of a ship to the flag of another Contracting Government, the Contracting Government whose flag the ship was formerly entitled to fly shall, as soon as possible, transmit to the receiving Administration copies of, or all information relating to, the International Ship Security Certificate carried by the ship before the transfer and copies of available verification reports, or

.2 A Company that assumes responsibility for the operation of a ship not previously operated by that Company, the previous Company shall as soon as possible, transmit to the receiving Company copies of any information related to the International Ship Security Certificate or to facilitate the verifications described in section 19.4.2.

19.4 Interim certification.

19.4.1 The certificates specified in section 19.2 shall be issued only when the Administration issuing the certificate is fully satisfied that the ship complies with the requirements of section 19.1. However, after 1 July 2004, for the purposes of:

.1 A ship without a certificate, on delivery or prior to its entry or re-entry into service;

.2 Transfer of a ship from the flag of a Contracting Government to the flag of another Contracting Government;

.3 Transfer of a ship to the flag of a Contracting Government from a State which is not a Contracting Government; or

.4 When a Company assumes the responsibility for the operation of a ship not previously operated by that Company; until the certificate referred to in section 19.2 is issued, the Administration may cause an Interim International Ship Security Certificate to be issued, in a form corresponding to the model given in the Appendix to this part of the Code.

19.4.2 An Interim International Ship Security Certificate shall only be issued when the Administration or recognized security organization, on behalf of the Administration, has verified that:

.1 The ship security assessment required by this part of the Code has been completed,

.2 A copy of the ship security plan meeting the requirements of chapter XI-2 and part A of this Code is provided on board, has been submitted for review and approval, and is being implemented on the ship;

.3 The ship is provided with a ship security alert system meeting the requirements of regulation XI-2/6, if required,

.4 The Company Security Officer:

.1 Has ensured:

.1 The review of the ship security plan for compliance with this part of the Code,

.2 That the plan has been submitted for approval, and

.3 That the plan is being implemented on the ship, and

.2 Has established the necessary arrangements, including arrangements for drills, exercises and internal audits, through which the Company Security Officer is satisfied that the ship will successfully complete the required verification in accordance with section 19.1.1.1, within 6 months;

.5 Arrangements have been made for carrying out the required verifications under section 19.1.1.1;

.6 The master, the ship's security officer and other ship's personnel with specific security duties are familiar with their duties and responsibilities as specified in this part of the Code; and with the relevant provisions of the ship security plan placed on board; and have been provided such information in the working language of the ship's personnel or languages understood by them; and

.7 The ship security officer meets the requirements of this part of the Code.

19.4.3 An Interim International Ship Security Certificate may be issued by the Administration or by a recognized security organization authorized to act on its behalf.

19.4.4 An Interim International Ship Security Certificate shall be valid for 6 months, or until the certificate required by section 19.2 is issued, whichever comes first, and may not be extended.

19.4.5 No Contracting Government shall cause a subsequent, consecutive Interim International Ship Security Certificate to be issued to a ship if, in the judgment of the Administration or the recognized security organization, one of the purposes of the ship or a Company in requesting such certificate is to avoid full compliance with chapter XI-2 and this part of the Code beyond the period of the initial interim certificate as specified in section 19.4.4.

19.4.6 For the purposes of regulation XI-2/9, Contracting Governments may, prior to accepting an Interim International Ship Security Certificate as a valid certificate, ensure that the requirements of sections 19.4.2.4 to 19.4.2.6 have been met.

Appendix to Part A

Appendix 1—Form of the International Ship Security Certificate

International Ship Security Certificate

(official seal)

(State)

Certificate No. _____

Issued under the provisions of the International Code for the Security of Ships and of Port Facilities (ISPS Code).

Under the authority of the Government of _____ (name of State) by _____ (persons or organization authorized)

Name of ship _____

Distinctive number or letters _____

Port of registry _____

Type of ship _____

Gross tonnage _____

IMO Number _____

Name and address of the Company _____

This is to certify:

1 That the security system and any associated security equipment of the ship has been verified in accordance with section 19.1 of part A of the ISPS Code;

2 That the verification showed that the security system and any associated security equipment of the ship is in all respects satisfactory and that the ship complies with the applicable requirements of chapter XI-2 of the Convention and part A of the ISPS Code;

3 That the ship is provided with an approved Ship Security Plan.

Date of initial / renewal verification on which this certificate is based _____

This Certificate is valid until _____ subject to verifications in accordance with section 19.1.1 of part A of the ISPS Code.

Issued at _____ (place of issue of the Certificate)

Date of issue _____

(signature of the duly authorized official issuing the Certificate)

(Seal or stamp of issuing authority, as appropriate)

Endorsement for Intermediate Verification

This is to certify that at an intermediate verification required by section 19.1.1 of part A of the ISPS Code the ship was found to comply with the relevant provisions of chapter XI-2 of the Convention and part A of the ISPS Code.

Intermediate Verification

Signed _____

(Signature of authorized official)

Place _____

Date _____

(Seal or stamp of the authority, as appropriate)

*Endorsement for Additional Verifications **

Additional Verification

Signed _____

(Signature of authorized official)

Place _____

Date _____

(Seal or stamp of the authority, as appropriate)

Additional Verification

Signed _____

(Signature of authorized official)

Place _____

Date _____

(Seal or stamp of the authority, as appropriate)

Additional Verification

Signed _____

(Signature of authorized official)

Place _____

Date _____

(Seal or stamp of the authority, as appropriate)

*This part of the certificate shall be adapted by the Administration to indicate

whether it has established additional verifications as provided for in section 19.1.1.4.

Additional Verification in Accordance With Section A/19.3.7.2 of the ISPS Code

This is to certify that at an additional verification required by section 19.3.7.2 of part A of the ISPS Code the ship was found to comply with the relevant provisions of chapter XI-2 of the Convention and part A of the ISPS Code.

Signed _____
(Signature of authorized official)
Place _____
Date _____
(Seal or stamp of the authority, as appropriate)

Endorsement to Extend the Certificate if Valid for Less Than 5 Years Where Section A/19.3.3 of the ISPS Code Applies

The ship complies with the relevant provisions of part A of the ISPS Code, and the Certificate shall, in accordance with section 19.3.3 of part A of the ISPS Code, be accepted as valid until _____.

Signed _____
(Signature of authorized official)
Place _____
Date _____
(Seal or stamp of the authority, as appropriate)

Endorsement Where the Renewal Verification Has Been Completed and Section A/19.3.4 of the ISPS Code Applies

The ship complies with the relevant provisions of part A of the ISPS Code, and the Certificate shall, in accordance with section 19.3.4 of part A of the ISPS Code, be accepted as valid until _____.

Signed _____
(Signature of authorized official)
Place _____
Date _____
(Seal or stamp of the authority, as appropriate)

Endorsement to Extend the Validity of the Certificate Until Reaching the Port of Verification Where Section A/19.3.5 of the ISPS Code Applies or for a Period of Grace Where Section A/19.3.6 of the ISPS Code Applies

This Certificate shall, in accordance with section 19.3.5/19.3.6 * of part A of the ISPS Code, be accepted as valid until _____.

Signed _____
(Signature of authorized official)
Place _____
Date _____
(Seal or stamp of the authority, as appropriate)

Endorsement for Advancement of Expiry Date Where Section A/19.3.7.1 of the ISPS Code Applies

In accordance with section 19.3.7.1 of part A of the ISPS Code, the new expiry date ** is _____.

Signed _____
(Signature of authorized official)
Place _____

Date _____
(Seal or stamp of the authority, as appropriate)

* Delete as appropriate.

**In case of completion of this part of the certificate the expiry date shown on the front of the certificate shall also be amended accordingly.

Appendix 2—Form of the Interim International Ship Security Certificate

Interim International Ship Security Certificate

(Official seal)

(State)

Certificate No. _____

Issued under the provisions of the International Code for the Security of Ships and of Port Facilities (ISPS Code)

Under the authority of the Government of _____ (name of State) by _____ (persons or organization authorized)

Name of ship: _____

Distinctive number or letters: _____

Port of registry: _____

Type of ship: _____

Gross tonnage: _____

IMO Number: _____

Name and address of company: _____

Is this a subsequent, consecutive interim certificate? Yes/No *

If Yes, date of issue of initial interim certificate _____

This is to certify that the requirements of section A/19.4.2 of the ISPS Code have been complied with.

This Certificate is issued pursuant to section A/19.4 * of the ISPS Code.

This Certificate is valid until _____.

Issued at _____ (place of issue of the certificate).

Date of issue _____

(signature of the duly authorized official issuing the Certificate)

(Seal or stamp of issuing authority, as appropriate)

*Delete as appropriate.

Part B

Guidance Regarding the Provisions of Chapter XI-2 of the Annex to the International Convention for the Safety of Life at Sea, 1974 as Amended and Part A of This Code

1 Introduction

General

1.1 The preamble of this Code indicates that chapter XI-2 and part A of this Code establish the new international framework of measures to enhance maritime security and through which ships and port facilities can co-operate to detect and deter acts which threaten security in the maritime transport sector.

1.2 This introduction outlines, in a concise manner, the processes envisaged in establishing and implementing the measures

and arrangements needed to achieve and maintain compliance with the provisions of chapter XI-2 and of part A of this Code and identifies the main elements on which guidance is offered. The guidance is provided in paragraphs 2 through to 19. It also sets down essential considerations, which should be taken into account when considering the application of the guidance relating to ships and port facilities.

1.3 If the reader's interest relates to ships alone, it is strongly recommended that this part of the Code is still read as a whole, particularly the sections relating to port facilities. The same applies to those whose primary interest are port facilities; they should also read the sections relating to ships.

1.4 The guidance provided in the following sections relates primarily to protection of the ship when it is at a port facility. There could, however, be situations when a ship may pose a threat to the port facility, e.g. because, once within the port facility, it could be used as a base from which to launch an attack. When considering the appropriate security measures to respond to ship-based security threats, those completing the Port Facility Security Assessment or preparing the Port Facility Security Plan should consider making appropriate adaptations to the guidance offered in the following sections.

1.5 The reader is advised that nothing in this Part of the Code should be read or interpreted in conflict with any of the provisions of either chapter XI-2 or part A of this Code and that the aforesaid provisions always prevail and override any unintended inconsistency which may have been inadvertently expressed in this Part of the Code. The guidance provided in this Part of the Code should always be read, interpreted and applied in a manner which is consistent with the aims, objectives and principles established in chapter XI-2 and part A of this Code.

Responsibilities of Contracting Governments

1.6 Contracting Governments have, under the provisions of chapter XI-2 and part A of this Code, various responsibilities, which, amongst others, include:

- Setting the applicable security level;
- Approving the Ship Security Plan and relevant amendments to a previously approved plan;
- Verifying the compliance of ships with the provisions of chapter XI-2 and part A of this Code and issuing to ships the International Ship Security Certificate;
- Determining which of the port facilities located within their territory are required to designate a Port Facility Security Officer who will be responsible for the preparation of the Port Facility Security Plan;
- Ensuring completion and approval of the Port Facility Security Assessment and of any subsequent amendments to a previously approved assessment;
- Approving the Port Facility Security Plan and any subsequent amendments to a previously approved plan; and
- Exercising control and compliance measures;
- Testing approved plans; and

—Communicating information to the International Maritime Organization and to the shipping and port industries.

1.7 Contracting Governments can designate, or establish, Designated Authorities within Government to undertake, with respect to port facilities, their security duties under chapter XI-2 and part A of this Code and allow Recognised Security Organisations to carry out certain work with respect to port facilities but the final decision on the acceptance and approval of this work should be given by the Contracting Government or the Designated Authority. Administrations may also delegate the undertaking of certain security duties, relating to ships, to Recognised Security Organizations. The following duties or activities cannot be delegated to a Recognized Security Organization:

- Setting of the applicable security level;
- Determining which of the port facilities located within the territory of a Contracting Government are required to designate a Port Facility Security Officer and to prepare a Port Facility Security Plan;
- Approving a Port Facility Security Assessment or any subsequent amendments to a previously approved assessment;
- Approving a Port Facility Security Plan or any subsequent amendments to a previously approved plan;
- Exercising control and compliance measures; and
- Establishing the requirements for a Declaration of Security.

Setting the Security Level

1.8 The setting of the security level applying at any particular time is the responsibility of Contracting Governments and can apply to ships and port facilities. Part A of this Code defines three security levels for international use. These are:

- Security Level 1, normal; the level at which ships and port facilities normally operate;
- Security Level 2, heightened; the level applying for as long as there is a heightened risk of a security incident; and
- Security Level 3, exceptional, the level applying for the period of time when there is the probable or imminent risk of a security incident.

The Company and the Ship

1.9 Any Company operating ships to which chapter XI-2 and part A of this Code apply has to designate a Company Security Officer for the Company and a Ship Security Officer for each of its ships. The duties, responsibilities and training requirements of these officers and requirements for drills, and exercises are defined in part A of this Code.

1.10 The Company Security Officer's responsibilities include, in brief amongst others, ensuring that a Ship Security Assessment is properly carried out, that a Ship Security Plan is prepared and submitted for approval by, or on behalf of, the Administration and thereafter is placed on board each ship to which part A of this Code applies and in respect of which that person has been appointed as the Company Security Officer.

1.11 The Ship Security Plan should indicate the operational and physical security measures the ship itself should take to ensure it always operates at security level 1.

The plan should also indicate the additional, or intensified, security measures the ship itself can take to move to and operate at security level 2 when instructed to do so.

Furthermore, the plan should indicate the possible preparatory actions the ship could take to allow prompt response to the instructions that may be issued to the ship by those responding at security level 3 to a security incident or threat thereof.

1.12 The ships to which the requirements of chapter XI-2 and part A of this Code apply are required to have, and operated in accordance with, a Ship Security Plan approved by, or on behalf of, the Administration. The Company and Ship Security Officer should monitor the continuing relevance and effectiveness of the plan, including the undertaking of internal audits. Amendments to any of the elements of an approved plan, for which the Administration has determined that approval is required, have to be submitted for review and approval before their incorporation in the approved plan and their implementation by the ship.

1.13 The ship has to carry an International Ship Security Certificate indicating that it complies with the requirements of chapter XI-2 and part A of this Code. Part A of this Code includes provisions relating to the verification and certification of the ship's compliance with the requirements on an initial, renewal and intermediate verification basis.

1.14 When a ship is at a port or is proceeding to a port of a Contracting Government, the Contracting Government has the right, under the provisions of regulation XI-2/9, to exercise various control and compliance measures with respect to that ship.

The ship is subject to port State control inspections but such inspections will not normally extend to examination of the Ship Security Plan itself except in specific circumstances.

The ship may, also, be subject to additional control measures if the Contracting Government exercising the control and compliance measures has reason to believe that the security of the ship has, or the port facilities it has served have, been compromised.

1.15 The ship is also required to have onboard information, to be made available to Contracting Governments upon request, indicating who is responsible for deciding the employment of the ship's personnel and for deciding various aspects relating to the employment of the ship.

The Port Facility

1.16 Each Contracting Government has to ensure completion of a Port Facility Security Assessment for each of the port facilities, located within its territory, serving ships engaged on international voyages. The Contracting Government, a Designated Authority or a Recognized Security Organization may carry out this assessment.

The completed Port Facility Security Assessment has to be approved by the Contracting Government or the Designated Authority concerned. This approval cannot be delegated. Port Facility Security Assessments should be periodically reviewed.

1.17 The Port Facility Security Assessment is fundamentally a risk analysis of all aspects of a port facility's operation in order to determine which part(s) of it are more susceptible, and/or more likely, to be the subject of attack. Security risk is a function of the threat of an attack coupled with the vulnerability of the target and the consequences of an attack.

The assessment must include the following components:

- The perceived threat to port installations and infrastructure must be determined;
- The potential vulnerabilities identified; and
- The consequences of incidents calculated.

On completion of the analysis, it will be possible to produce an overall assessment of the level of risk. The Port Facility Security Assessment will help determine which port facilities are required to appoint a Port Facility Security Officer and prepare a Port Facility Security Plan.

1.18 The port facilities which have to comply with the requirements of chapter XI-2 and part A of this Code are required to designate a Port Facility Security Officer. The duties, responsibilities and training requirements of these officers and requirements for drills and exercises are defined in part A of this Code.

1.19 The Port Facility Security Plan should indicate the operational and physical security measures the port facility should take to ensure that it always operates at security level 1. The plan should also indicate the additional, or intensified, security measures the port facility can take to move to and operate at security level 2 when instructed to do so.

Furthermore, the plan should indicate the possible preparatory actions the port facility could take to allow prompt response to the instructions that may be issued by those responding at security level 3 to a security incident or threat thereof.

1.20 The port facilities which have to comply with the requirements of chapter XI-2 and part A of this Code are required to have, and operate in accordance with, a Port Facility Security Plan approved by the Contracting Government or by the Designated Authority concerned.

The Port Facility Security Officer should implement its provisions and monitor the continuing effectiveness and relevance of the plan, including commissioning internal audits of the application of the plan.

Amendments to any of the elements of an approved plan, for which the Contracting Government or the Designated Authority concerned has determined that approval is required, have to be submitted for review and approval before their incorporation in the approved plan and their implementation at the port facility.

The Contracting Government or the Designated Authority concerned may test the effectiveness of the plan. The Port Facility

Security Assessment covering the port facility or on which the development of the plan has been based should be regularly reviewed. All these activities may lead to amendment of the approved plan. Any amendments to specified elements of an approved plan will have to be submitted for approval by the Contracting Government or by the Designated Authority concerned.

1.21 Ships using port facilities may be subject to the port State control inspections and additional control measures outlined in regulation XI-2/9.

The relevant authorities may request the provision of information regarding the ship, its cargo, passengers and ship's personnel prior to the ship's entry into port.

There may be circumstances in which entry into port could be denied.

Information and Communication

1.22 Chapter XI-2 and part A of this Code require Contracting Governments to provide certain information to the International Maritime Organization and for information to be made available to allow effective communication between Contracting Governments and between Company/Ship Security Officers and the Port Facility Security Officers responsible for the port facility their ships visit.

2 Definitions

2.1 No guidance is provided with respect to the definitions set out in chapter XI-2 or part A of this Code.

2.2 For the purpose of this part of the Code:

.1 "Section" means a section of part A of the Code and is indicated as "section A/<followed by the number of the section>";

.2 "Paragraph" means a paragraph of this part of the Code and is indicated as "paragraph <followed by the number of the paragraph>"; and

.3 "*Contracting Government*", when used in paragraphs 14 to 18, means the "Contracting Government within whose territory the port facility is located" and includes a reference to the "Designated Authority".

3 Application

General

3.1 The guidance given in this part of the Code should be taken into account when implementing the requirements of chapter XI-2 and part A of this Code.

3.2 However, it should be recognized that the extent to which the guidance on ships applies will depend on the type of ship, its cargoes and/or passengers, its trading pattern and the characteristics of the port facilities visited by the ship.

3.3 Similarly, in relation to the guidance on port facilities, the extent to which this guidance applies will depend on the port facilities, the types of ships using the port facility, the types of cargo and/or passengers and the trading patterns of visiting ships.

3.4 The provisions of chapter XI-2 and part A of this Code are not intended to apply to port facilities designed and used primarily for military purposes.

4 Responsibility of Contracting Governments

Security of Assessments and Plans

4.1 Contracting Governments should ensure that appropriate measures are in place to avoid unauthorized disclosure of, or access to, security sensitive material relating to Ship Security Assessments, Ship Security Plans, Port Facility Security Assessments and Port Facility Security Plans, and to individual assessments or plans.

Designated Authorities

4.2 Contracting Governments may identify a Designated Authority within Government to undertake their security duties relating to port facilities as set out in chapter XI-2 or part A of this Code.

Recognized Security Organizations

4.3 Contracting Governments may authorize a Recognized Security Organization (RSO) to undertake certain security related activities, including:

.1 Approval of Ship Security Plans, or amendments thereto, on behalf of the Administration;

.2 Verification and certification of compliance of ships with the requirements of chapter XI-2 and part A of this Code on behalf of the Administration; and

.3 Conducting Port Facility Security Assessments required by the Contracting Government.

4.4 An RSO may also advise or provide assistance to Companies or port facilities on security matters, including Ship Security Assessments, Ship Security Plans, Port Facility Security Assessments and Port Facility Security Plans. This can include completion of a Ship Security Assessment or Plan or Port Facility Security Assessment or Plan.

If an RSO has done so in respect of a ship security assessment or plan that RSO should not be authorised to approve that ship security plan.

4.5 When authorizing an RSO, Contracting Governments should give consideration to the competency of such an organization. An RSO should be able to demonstrate:

.1 Expertise in relevant aspects of security;

.2 Appropriate knowledge of ship and port operations, including knowledge of ship design and construction if providing services in respect of ships and port design and construction if providing services in respect of port facilities;

.3 Their capability to assess the likely security risks that could occur during ship and port facility operations including the ship/port interface and how to minimise such risks;

.4 Their ability to maintain and improve the expertise of their personnel;

.5 Their ability to monitor the continuing trustworthiness of their personnel;

.6 Their ability to maintain appropriate measures to avoid unauthorised disclosure of, or access to, security sensitive material;

.7 Their knowledge of the requirements chapter XI-2 and part A of this Code and relevant national and international legislation and security requirements; and

.8 Their knowledge of current security threats and patterns;

.9 Their knowledge on recognition and detection of weapons, dangerous substances and devices;

.10 Their knowledge on recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

.11 Their knowledge on techniques used to circumvent security measures; and

.12 Their knowledge of security and surveillance equipment and systems and their operational limitations.

When delegating specific duties to an RSO, Contracting Governments, including Administrations, should ensure that the RSO has the competencies needed to undertake the task.

4.6 A Recognized Organization, as defined in regulation I/6 and fulfilling the requirements of regulation XI-1/1, may be appointed as a RSO provided it has the appropriate security related expertise listed in paragraph 4.5.

4.7 A Port or Harbour Authority or Port Facility operator may be appointed as an RSO provided it has the appropriate security related expertise listed in paragraph 4.5.

Setting the Security Level

4.8 In setting the security level Contracting Governments should take account of general and specific threat information. Contracting Governments should set the security level applying to ships or port facilities at one of three levels:

- Security level 1: normal, the level at which the ship or port facility normally operates;
- Security level 2: heightened, the level applying for as long as there is a heightened risk of a security incident; and
- Security level 3: exceptional, the level applying for the period of time when there is the probable or imminent risk of a security incident.

4.9 Setting security level 3 should be an exceptional measure applying only when there is credible information that a security incident is probable or imminent.

Security level 3 should only be set for the duration of the identified security threat or actual security incident.

While the security levels may change from security level 1, through security level 2 to security level 3, it is also possible that the security levels will change directly from security level 1 to security level 3.

4.10 At all times the Master of a ship has the ultimate responsibility for the safety of the ship. Even at security level 3 a Master may seek clarification or amendment of instructions issued by those responding to a security incident, or threat thereof, if there are reasons to believe that compliance with any instruction may imperil the safety of the ship.

4.11 The Company Security Officer (CSO) or the Ship Security Officer (SSO) should liaise at the earliest opportunity with the Port Facility Security Officer (PFSO) of the port facility the ship is intended to visit to establish the security level applying for that ship at the port facility. Having established contact with a ship, the PFSO should advise the ship of any subsequent change in the port

facility's security level and should provide the ship with any relevant security information.

4.12 While there may be circumstances when an individual ship may be operating at a higher security level than the port facility it is visiting, there will be no circumstances when a ship can have a lower security level than the port facility it is visiting. If a ship has a higher security level than the port facility it intends to use, the CSO or SSO should advise the PFSP without delay. The PFSP should undertake an assessment of the particular situation in consultation with the CSO or SSO and agree on appropriate security measures with the ship, which may include completion and signing of a Declaration of Security.

4.13 Contracting Governments should consider how information on changes in security levels should be promulgated rapidly. Administrations may wish to use NAVTEX messages or Notices to Mariners as the method for notifying such changes in security levels to ship and CSO and SSO. Or, they may wish to consider other methods of communication that provide equivalent or better speed and coverage. Contracting Governments should establish means of notifying PFSPs of changes in security levels.

Contracting Governments should compile and maintain the contact details for a list of those who need to be informed of changes in security levels. Whereas the security level need not be regarded as being particularly sensitive, the underlying threat information may be highly sensitive. Contracting Governments should give careful consideration to the type and detail of the information conveyed and the method by which it is conveyed, to SSOs, CSOs and PFSPs.

Contact Points and Information on Port Facility Security Plans

4.14 Where a port facility has a PFSP that fact has to be communicated to the Organization and that information must also be made available to Company and Ship Security Officers. No further details of the PFSP have to be published other than that it is in place. Contracting Governments should consider establishing either central or regional points of contact, or other means of providing up to date information on the locations where PFSPs are in place, together with contact details for the relevant PFSP. The existence of such contact points should be publicised. They could also provide information on the recognized security organizations appointed to act on behalf of the Contracting Government, together with details of the specific responsibility and conditions of authority delegated to such recognised security organizations.

4.15 In the case of a port that does not have a PFSP (and therefore does not have a PFSP) the central or regional point of contact should be able to identify a suitably qualified person ashore who can arrange for appropriate security measures to be in place, if needed, for the duration of the ship's visit.

4.16 Contracting Governments should also provide the contact details of Government officers to whom an SSO, a CSO and a PFSP can report security concerns.

These Government officers should assess such reports before taking appropriate action. Such reported concerns may have a bearing on the security measures falling under the jurisdiction of another Contracting Government. In that case, the Contracting Governments should consider contacting their counterpart in the other Contracting Government to discuss whether remedial action is appropriate. For this purpose, the contact details of the Government officers should be communicated to the International Maritime Organization.

4.17 Contracting Governments should also make the information indicated in paragraphs 4.14 to 4.16, available to other Contracting Governments on request.

Identification Documents

4.18 Contracting Governments are encouraged to issue appropriate identification documents to Government officials entitled to board ships or enter port facilities when performing their official duties and to establish procedures whereby the authenticity of such documents might be verified.

Fixed and Floating Platforms and Mobile Drilling Units on Location

4.19 Contracting Governments should consider establishing appropriate security measures for fixed and floating platforms and mobile offshore drilling units on location to allow interaction with ships which are required to comply with the provisions of chapter XI-2 and part A of this Code¹.

Ships Which Are Not Required To Comply With Part A of This Code

4.20 Contracting Governments should consider establishing appropriate security measures to enhance the security of ships to which this chapter XI-2 and part A of this Code does not apply and to ensure that any security provisions applying to such ships allow interaction with ships to which part A of this Code applies.

Threats to Ships and Other Incidents at Sea

4.21 Contracting Governments should provide general guidance on the measures considered appropriate to reduce the security risk to ships flying their flag when at sea. They should provide specific advice on the action to be taken in accordance with security levels 1 to 3, if:

- .1 There is a change in the security level applying to the ship while it is at sea, e.g. because of the geographical area in which it is operating or relating to the ship itself; and
- .2 There is a security incident or threat thereof involving the ship while at sea.

Contracting Governments should establish the best methods and procedures for these purposes. In the case of an imminent attack the ship should seek to establish direct communication with those responsible in the flag State for responding to security incidents.

¹ Refer to Establishment of Appropriate Measures to Enhance the Security of Ships, Port Facilities, Mobile Offshore Drilling Units on location and Fixed and Floating Platforms Not Covered by chapter XI-2 of 1974 SOLAS Convention, adopted by the Conference on Maritime Security by resolution 7.

4.22 Contracting Governments should also establish a point of contact for advice on security for any ship:

- .1 Entitled to fly their flag; or
- .2 Operating in their territorial sea or having communicated an intention to enter their territorial sea.

4.23 Contracting Governments should offer advice to ships operating in their territorial sea or having communicated an intention to enter their territorial sea, which could include advice:

- .1 To alter or delay their intended passage;
- .2 To navigate on a particular course or proceed to a specific location;
- .3 On the availability of any personnel or equipment that could be placed on the ship;
- .4 To co-ordinate the passage, arrival into port or departure from port, to allow escort by patrol craft or aircraft (fixed-wing or helicopter).

Contracting Governments should remind ships operating in their territorial sea, or having communicated an intention to enter their territorial sea, of any temporary restricted areas that they have published.

4.24 Contracting Governments should recommend that ships operating in their territorial sea, or having communicated an intention to enter their territorial sea, implement expeditiously, for the ship's protection and for the protection of other ships in the vicinity, any security measure the Contracting Government may have advised.

4.25 The plans prepared by the Contracting Governments for the purposes given in paragraph 4.22 should include information on an appropriate point of contact, available on a 24-hour basis, within the Contracting Government including the Administration. These plans should also include information on the circumstances in which the Administration considers assistance should be sought from nearby coastal States, and a procedure for liaison between port facility security officers and ship security officers.

Alternative Security Agreements

4.26 Contracting Governments, in considering how to implement chapter XI-2 and part A of this Code, may conclude one or more agreements with one or more Contracting Governments. The scope of an agreement is limited to short international voyages on fixed routes between port facilities in the territory of the parties to the agreement.

When concluding an agreement, and thereafter, the Contracting Governments should consult other Contracting Governments and Administrations with an interest in the effects of the agreement. Ships flying the flag of a State that is not party to the agreement should only be allowed to operate on the fixed routes covered by the agreement if their Administration agrees that the ship should comply with the provisions of the agreement and requires the ship to do so.

In no case can such an agreement compromise the level of security of other ships and port facilities not covered by it, and specifically, all ships covered by such an agreement may not conduct ship-to-ship

activities with ships not so covered. Any operational interface undertaken by ships covered by the agreement should be covered by it.

The operation of each agreement must be continually monitored and amended when the need arises and in any event should be reviewed every 5 years.

Equivalent Arrangements for Port Facilities

4.27 For certain specific port facilities with limited or special operations but with more than occasional traffic, it may be appropriate to ensure compliance by security measures equivalent to those prescribed in chapter XI-2 and in part A of this Code. This can, in particular, be the case for terminals such as those attached to factories, or quaysides with no frequent operations."

Manning Level

4.28 In establishing the minimum safe manning of a ship the Administration should take into account² that the minimum safe manning provisions established by regulation V/14³ only address the safe navigation of the ship. The Administration should also take into account any additional workload which may result from the implementation of the ship's security plan and ensure that the ship is sufficiently and effectively manned. In doing so the Administration should verify that ships are able to implement the hours of rest and other measures to address fatigue which have been promulgated by national law, in the context of all shipboard duties assigned to the various shipboard personnel.

Control and Compliance Measures⁴

General

4.29 Regulation XI-2/9 describes the control and compliance measures applicable to ships under chapter XI-2. It is divided into three distinct sections; control of ships already in a port, control of ships intending to enter a port of another Contracting Government, and additional provisions applicable to both situations.

4.30 Regulation XI-2/9.1, control of ships in port, implements a system for the control of ships while in the port of a foreign country where duly authorized officers of the Contracting Government (duly authorized officers) have the right to go on board the ship to verify that the required certificates are in proper order. Then if there are clear grounds to believe the ship does not comply, control measures such as additional inspections or detention may be taken. This reflects current control systems.⁵

² Refer to Further Work by the International Maritime Organisation pertaining to Enhancement of Maritime Security, adopted by the Conference on Maritime Security by resolution 3, inviting, amongst others, the Organisation to review Assembly Resolution A.890(21) on Principles of Safe Manning. This review may also lead to amendments of regulation V/14.

³ As was in force on the date of adoption of this Code.

⁴ Refer to Further Work by the International Maritime Organisation pertaining to Enhancement of Maritime Security, adopted by the Conference on Maritime Security by resolution 3, inviting, amongst others, the Organisation to review Assembly Resolutions A.787(19) and A.822(21).

⁵ See regulation I/19 and regulation IX/6.2 of SOLAS 74 as amended, article 21 of LOADLINE 66

Regulation XI-2/9.1 builds on such systems and allows for additional measures (including expulsion of a ship from a port to be taken as a control measure) when duly authorized officers have clear grounds for believing that a ship is in non-compliance with the requirements of chapter XI-2 or part A of this Code. Regulation XI-2/9.3 describes the safeguards that promote fair and proportionate implementation of these additional measures.

4.31 Regulation XI-2/9.2 applies control measures to ensure compliance to ships intending to enter a port of another Contracting Government and introduces an entirely different concept of control within chapter XI-2, applying to security only. Under this regulation measures may be implemented prior to the ship entering port, to better ensure security. Just as in regulation XI-2/9.1, this additional control system is based on the concept of clear grounds for believing the ship does not comply with chapter XI-2 or part A of this Code, and includes significant safeguards in regulations XI-2/9.2.2 and XI-2/9.2.5 as well as in regulation XI-2/9.3.

4.32 Clear grounds that the ship is not in compliance means evidence or reliable information that the ship does not correspond with the requirements of chapter XI-2 or part A of this Code, taking into account the guidance given in this part of the Code. Such evidence or reliable information may arise from the duly authorized officer's professional judgement or observations gained while verifying the ship's International Ship Security Certificate or Interim International Ship Security Certificate issued in accordance with part A of this Code (certificate) or from other sources. Even if a valid certificate is on board the ship, the duly authorized officers may still have clear grounds for believing that the ship is not in compliance based on their professional judgment.

4.33 Examples of possible clear grounds under regulations XI-2/9.1 and XI-2/9.2 may include, when relevant:

.1 Evidence from a review of the certificate that it is not valid or it has expired;

.2 Evidence or reliable information that serious deficiencies exist in the security equipment, documentation or arrangements required by chapter XI-2 and part A of this Code;

.3 Receipt of a report or complaint which, in the professional judgment of the duly authorized officer, contains reliable information clearly indicating that the ship does not comply with the requirements of chapter XI-2 or part A of this Code;

.4 Evidence or observation gained by a duly authorized officer using professional judgment that the master or ship's personnel is not familiar with essential shipboard security procedures or cannot carry out drills related to the security of the ship or that such

procedures or drills have not been carried out;

.5 Evidence or observation gained by a duly authorized officer using professional judgment that key members ship's personnel are not able to establish proper communication with any other key members of ship's personnel with security responsibilities on board the ship;

.6 Evidence or reliable information that the ship has embarked persons, or loaded stores or goods at a port facility or from another ship where either the port facility or the other ship is in violation of chapter XI-2 or part A of this Code, and the ship in question has not completed a Declaration of Security, nor taken appropriate, special or additional security measures or has not maintained appropriate ship security procedures;

.7 Evidence or reliable information that the ship has embarked persons, or loaded stores or goods at a port facility or from another source (e.g., another ship or helicopter transfer) where either the port facility or the other source is not required to comply with chapter XI-2 or part A of this Code, and the ship has not taken appropriate, special or additional security measures or has not maintained appropriate security procedures; and

.8 If the ship holds a subsequent, consecutively issued Interim International Ship Security Certificate as described in section A/19.4, and if, in the professional judgment of an officer duly authorized, one of the purposes of the ship or a Company in requesting such certificate is to avoid full compliance with chapter XI-2 and part A of this Code beyond the period of the initial interim certificate as described in section A/19.4.4.

4.34 The international law implications of regulation XI-2/9 are particularly relevant, and the regulation should be implemented with regulation XI-2/2.4 in mind, as the potential exists for situations where either measures will be taken which fall outside the scope of chapter XI-2, or where rights of affected ships, outside chapter XI-2, should be considered. Thus, regulation XI-2/9 does not prejudice the Contracting Government from taking measures having a basis in, and consistent with, international law, to ensure the safety or security of people, ships, port facilities and other property in cases where the ship, although in compliance with chapter XI-2 and part A of this Code, is still considered to present a security risk.

4.35 When a Contracting Government imposes control measures on a ship, the Administration should, without delay, be contacted with sufficient information to enable the Administration to fully liaise with the Contracting Government.

Control of Ships in Port

4.36 Where the non-compliance is either a defective item of equipment or faulty documentation leading to the ship's detention and the non-compliance cannot be remedied in the port of inspection, the Contracting Government may allow the ship to sail to another port provided that any conditions agreed between the port States and the Administration or master are met.

as modified by the 1988 LOADLINE Protocol, articles 5 and 6, regulation 8A of Annex I, regulation 15 of Annex II of MARPOL 73/78 as amended, article X of STCW 78 as amended and IMO Assembly Resolutions A.787(19) and A.882(21).

Ships Intending To Enter the Port of Another Contracting Government

4.37 Regulation XI-2/9.2.1 lists the information Contracting Governments may require from a ship as a condition of entry into port. One item of information listed is confirmation of any special or additional measures taken by the ship during its last ten calls at a port facility. Examples could include:

.1 Records of the measures taken while visiting a port facility located in the territory of a State which is not a Contracting Government especially those measures that would normally have been provided by port facilities located in the territories of Contracting Governments; and

.2 Any Declarations of Security that were entered into with port facilities or other ships.

4.38 Another item of information listed, that may be required as a condition of entry into port, is confirmation that appropriate ship security procedures were maintained during ship-to-ship activity conducted within the period of the last 10 calls at a port facility. It would not normally be required to include records of transfers of pilots, customs, immigration, security officials nor bunkering, lightering, loading of supplies and unloading of waste by ship within port facilities as these would normally fall within the auspices of the Port Facility Security Plan. Examples of information that might be given include:

.1 Records of the measures taken while engaged in a ship to ship activity with a ship flying the flag of a State which is not a Contracting Government especially those measures that would normally have been provided by ships flying the flag of Contracting Governments;

.2 Records of the measures taken while engaged in a ship to ship activity with a ship that is flying the flag of a Contracting Government but is not required to comply with the provisions of chapter XI-2 and part A of this Code such as a copy of any security certificate issued to that ship under other provisions; and

.3 In the event that persons or goods rescued at sea are on board, all known information about such persons or goods, including their identities when known and the results of any checks run on behalf of the ship to establish the security status of those rescued. It is not the intention of chapter XI-2 or part A of this Code to delay or prevent the delivery of those in distress at sea to a place of safety. It is the sole intention of chapter XI-2 and part A of this Code to provide States with enough appropriate information to maintain their security integrity.

4.39 Examples of other practical security related information that may be required as a condition of entry into port in order to assist with ensuring the safety and security of persons, port facilities, ships and other property include:

.1 Information contained in the Continuous Synopsis Record;

.2 Location of the ship at the time the report is made;

.3 Expected time of arrival of the ship in port;

.4 Crew list;

.5 General description of cargo aboard the ship;

.6 Passenger list; and

.7 Information required to be carried under regulation XI-2/10.

4.40 Regulation XI-2/9.2.5 allows the master of a ship, upon being informed that the coastal or port State will implement control measures under regulation XI-2/9.2, to withdraw the intention for the ship to enter port. If the master withdraws that intention, regulation XI-2/9 no longer applies, and any other steps that are taken must be based on, and consistent with, international law.

Additional Provisions

4.41 In all cases where a ship is denied entry or expelled from a port, all known facts should be communicated to the authorities of relevant States. This communication should consist of the following when known:

.1 Name of ship, its flag, the ship's identification number, call sign, ship type and cargo;

.2 Reason for denying entry or expulsion from port or port areas;

.3 If relevant, the nature of any security non-compliance;

.4 If relevant, details of any attempts made to rectify any non-compliance, including any conditions imposed on the ship for the voyage;

.5 Past port(s) of call and next declared port of call;

.6 Time of departure and likely estimated time of arrival at those ports;

.7 Any instructions given to ship, e.g., reporting on route;

.8 Available information on the security level at which the ship is currently operating;

.9 Information regarding any communications the port State has had with the Administration;

.10 Contact point within the port State making the report for the purpose of obtaining further information;

.11 Crew list; and

.12 Any other relevant information.

4.42 Relevant States to contact should include those along the ship's intended passage to its next port, particularly if the ship intends to enter the territorial sea of that coastal State. Other relevant States could include previous ports of call, so that further information might be obtained and security issues relating to the previous ports resolved.

4.43 In exercising control and compliance measures, the duly authorized officers should ensure that any measures or steps imposed are proportionate. Such measures or steps should be reasonable and of the minimum severity and duration necessary to rectify or mitigate the non-compliance.

4.44 The word "delay" in regulation XI-2/9.3.3.1 also refers to situations where, pursuant to actions taken under this regulation, the ship is unduly denied entry into port or the ship is unduly expelled from port.

Non-Party Ships and Ships Below Convention Size

4.45 With respect to ships flying the flag of a State which is not a Contracting Government to the Convention and not a

Party to the 1988 SOLAS Protocol⁶, Contracting Governments should not give more favourable treatment to such ships. Accordingly, the requirements of regulation XI-2/9 and the guidance provided in this Part of the Code should be applied to those ships.

4.46 Ships below Convention size are subject to measures by which States maintain security. Such measures should be taken with due regard to the requirements in chapter XI-2 and the guidance provided in this Part of the Code.

5 Declaration of Security

General

5.1 A Declaration of Security (DoS) should be completed when the Contracting Government of the port facility deems it to be necessary or when a ship deems it necessary.

5.1.1 The need for a DoS may be indicated by the results of the Port Facility Security Assessment (PFA) and the reasons and circumstances in which a DoS is required should be set out in the Port Facility Security Plan (PFSP).

5.1.2 The need for a DoS may be indicated by an Administration for ships entitled to fly its flag or as a result of a ship security assessment and should be set out in the ship security plan.

5.2 It is likely that a DoS will be requested at higher security levels, when a ship has a higher security level than the port facility, or another ship with which it interfaces, and for ship/port interface or ship to ship activities that pose a higher risk to persons, property or the environment for reasons specific to that ship, including its cargo or passengers or the circumstances at the port facility or a combination of these factors.

5.2.1 In the case that a ship or an Administration, on behalf of ships entitled to fly its flag, requests completion of a DoS, the Port Facility Security Officer (PFSO) or Ship Security Officer (SSO) should acknowledge the request and discuss appropriate security measures.

5.3 A PFSO may also initiate a DoS prior to ship/port interfaces that are identified in the approved PFA as being of particular concern. Examples may include the embarking or disembarking passengers, and the transfer, loading or unloading of dangerous goods or hazardous substances.

The PFA may also identify facilities at or near highly populated areas or economically significant operations that warrant a DoS.

5.4 The main purpose of a DoS is to ensure agreement is reached between the ship and the port facility or with other ships with which it interfaces as to the respective security measures each will undertake in accordance with the provisions of their respective approved security plans.

5.4.1 The agreed DoS should be signed and dated by both the port facility and the ship(s), as applicable, to indicate compliance with chapter XI-2 and part A of this Code and should include its duration, the relevant security level, or levels and the contact points.

⁶Protocol of 1988 relating to the International Convention for the Safety of Life at Sea, 1974.

5.4.2 A change in the security level may require that a new or revised DoS be completed.

5.5 The DoS should be completed in English, French or Spanish or in a language common to both the port facility and the ship or the ships, as applicable.

5.6 A model DoS is included in Appendix 1 to this part of the Code.

6 Obligations of the Company

6.1 Regulation XI-2/5 requires the company to provide the master of the ship with information to meet the requirements of the Company under the provisions of this regulation. This information should include items such as:

.1 Parties responsible for appointing shipboard personnel, such as ship management companies, manning agents, contractors, concessionaries, for example, retail sales outlets, casinos etc;

.2 Parties responsible for deciding the employment of the ship including, time or bareboat charterer(s) or any other entity acting in such capacity; and

.3 In cases when the ship is employed under the terms of a charter party, the contact details of those parties including time or voyage charterers

6.2 In accordance with regulation XI-2/5 the Company is obliged to update and keep this information current as and when changes occur.

6.3 This information should be in English, French or Spanish language.

6.4 With respect to ships constructed before July 1, 2004, this information should reflect the actual condition on that date.

6.5 With respect to ships constructed on or after July 1, 2004, and for ships constructed before July 1, 2004, which were out of service on July 1, 2004, the information should be provided as from the date of entry of the ship into service and should reflect the actual condition on that date.

6.6 After July 1, 2004, when a ship is withdrawn from service the information should be provided as from the date of re-entry of the ship into service and should reflect the actual condition on that date.

6.7 Previously provided information that does not relate to the actual condition on that date need not be retained on board.

6.8 When the responsibility for the operation of the ship is assumed by another Company, the information relating to the Company, which operated the ship, are not required to be left on board.

In addition other relevant guidance is provided under sections 8, 9 and 13.

7 Ship Security

Relevant guidance is provided under sections 8, 9 and 13.

8 Ship Security Assessment

Security Assessment

8.1 The Company Security Officer (CSO) is responsible for ensuring that a Ship Security Assessment (SSA) is carried out for each of the ships in the Company's fleet which is required to comply with the provisions of chapter XI-2 and part A of this Code for which the CSO is responsible. While the CSO need not necessarily

personally undertake all the duties associated with the post, the ultimate responsibility for ensuring that they are properly performed remains with the individual CSO.

8.2 Prior to commencing the SSA, the CSO should ensure that advantage is taken of information available on the assessment of threat for the ports at which the ship will call or at which passengers embark or disembark and about the port facilities and their protective measures. The CSO should study previous reports on similar security needs.

Where feasible, the CSO should meet with appropriate persons on the ship and in the port facilities to discuss the purpose and methodology of the assessment.

The CSO should follow any specific guidance offered by the Contracting Governments.

8.3 A SSA should address the following elements on board or within the ship:

- .1 Physical security;
- .2 Structural integrity;
- .3 Personnel protection systems;
- .4 Procedural policies;
- .5 Radio and telecommunication systems, including computer systems and networks;

.6 Other areas that may, if damaged or used for illicit observation, pose a risk to people, property, or operations on board the ship or within a port facility.

8.4 Those involved in a SSA should be able to draw upon expert assistance in relation to:

- .1 Knowledge of current security threats and patterns;
- .2 Recognition and detection of weapons, dangerous substances and devices;
- .3 Recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;
- .4 Techniques used to circumvent security measures;
- .5 Methods used to cause a security incident;
- .6 Effects of explosives on ship's structures and equipment;
- .7 Ship security;
- .8 Ship/port interface business practices;
- .9 Contingency planning, emergency preparedness and response;
- .10 Physical security;
- .11 Radio and telecommunications systems, including computer systems and networks;
- .12 Marine engineering; and
- .13 Ship and port operations.

8.5 The CSO should obtain and record the information required to conduct an assessment, including:

- .1 The general layout of the ship;
- .2 The location of areas which should have restricted access, such as navigation bridge, machinery spaces of category A and other control stations as defined in chapter II-2, etc.;
- .3 The location and function of each actual or potential access point to the ship;
- .4 Changes in the tide which may have an impact on the vulnerability or security of the ship;
- .5 The cargo spaces and stowage arrangements;
- .6 The locations where the ship's stores and essential maintenance equipment is stored;

.7 The locations where unaccompanied baggage is stored;

.8 The emergency and stand-by equipment available to maintain essential services;

.9 The number of ship's personnel, any existing security duties and any existing training requirement practises of the Company;

.10 Existing security and safety equipment for the protection of passengers and ship's personnel;

.11 Escape and evacuation routes and assembly stations which have to be maintained to ensure the orderly and safe emergency evacuation of the ship;

.12 Existing agreements with private security companies providing ship/waterside security services; and

.13 Existing security measures and procedures in effect, including inspection and, control procedures, identification systems, surveillance and monitoring equipment, personnel identification documents and communication, alarms, lighting, access control and other appropriate systems.

8.6 The SSA should examine each identified point of access, including open weather decks, and evaluate its potential for use by individuals who might seek to breach security. This includes points of access available to individuals having legitimate access as well as those who seek to obtain unauthorized entry.

8.7 The SSA should consider the continuing relevance of the existing security measures and guidance, procedures and operations, under both routine and emergency conditions and should determine security guidance including:

- .1 The restricted areas;
- .2 The response procedures to fire or other emergency conditions;
- .3 The level of supervision of the ship's personnel, passengers, visitors, vendors, repair technicians, dock workers, etc.;
- .4 The frequency and effectiveness of security patrols;
- .5 The access control systems, including identification systems;
- .6 The security communications systems and procedures;
- .7 The security doors, barriers and lighting; and
- .8 The security and surveillance equipment and systems, if any.

8.8 The SSA should consider the persons, activities, services and operations that it is important to protect. This includes:

- .1 The ship's personnel;
- .2 Passengers, visitors, vendors, repair technicians, port facility personnel, etc.;
- .3 The capacity to maintain safe navigation and emergency response;
- .4 The cargo, particularly dangerous goods or hazardous substances;
- .5 The ship's stores;
- .6 The ship security communication equipment and systems, if any; and
- .7 The ship's security surveillance equipment and systems, if any.

8.9 The SSA should consider all possible threats, which may include the following types of security incidents:

.1 Damage to, or destruction of, the ship or of a port facility, *e.g.* by explosive devices, arson, sabotage or vandalism;

.2 Hijacking or seizure of the ship or of persons on board;

.3 Tampering with cargo, essential ship equipment or systems or ship's stores;

.4 Unauthorized access or use, including presence of stowaways;

.5 Smuggling weapons or equipment, including weapons of mass destruction;

.6 Use of the ship to carry those intending to cause a security incident and/or their equipment;

.7 Use of the ship itself as a weapon or as a means to cause damage or destruction;

.8 Attacks from seaward whilst at berth or at anchor; and

.9 Attacks whilst at sea.

8.10 The SSA should take into account all possible vulnerabilities, which may include:

.1 Conflicts between safety and security measures;

.2 Conflicts between shipboard duties and security assignments;

.3 Watch-keeping duties, number of ship's personnel, particularly with implications on crew fatigue, alertness and performance;

.4 Any identified security training deficiencies; and

.5 Any security equipment and systems, including communication systems.

8.11 The CSO and SSO should always have regard to the effect that security measures may have on ship's personnel who will remain on the ship for long periods. When developing security measures, particular consideration should be given to the convenience, comfort and personal privacy of the ship's personnel and their ability to maintain their effectiveness over long periods.

8.12 Upon completion of the SSA, a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment and a description of counter measures that could be used to address each vulnerability. The report shall be protected from unauthorized access or disclosure.

8.13 If the SSA has not been carried out by the Company the report of the SSA should be reviewed and accepted by the CSO.

On-scene Security Survey

8.14 The on-scene security survey is an integral part of any SSA. The on-scene security survey should examine and evaluate existing shipboard protective measures, procedures and operations for:

.1 Ensuring the performance of all ship security duties;

.2 Monitoring restricted areas to ensure that only authorized persons have access;

.3 Controlling access to the ship, including any identification systems;

.4 Monitoring of deck areas and areas surrounding the ship;

.5 Controlling the embarkation of persons and their effects (accompanied and unaccompanied baggage and ship's personnel personal effects);

.6 Supervising the handling of cargo and the delivery of ship's stores; and

.7 Ensuring that ship security communication, information, and equipment are readily available.

9 Ship Security Plan

General

9.1 The Company Security Officer (CSO) has the responsibility of ensuring that a Ship Security Plan (SSP) is prepared and submitted for approval. The content of each individual SSP should vary depending on the particular ship it covers. The Ship Security Assessment (SSA) will have identified the particular features of the ship and the potential threats and vulnerabilities. The preparation of the SSP will require these features to be addressed in detail. Administrations may prepare advice on the preparation and content of a SSP.

9.2 All SSPs should:

.1 Detail the organizational structure of security for the ship;

.2 Detail the ship's relationships with the Company, port facilities, other ships and relevant authorities with security responsibility;

.3 Detail the communication systems to allow effective continuous communication within the ship and between the ship and others, including port facilities;

.4 Detail the basic security measures for security level 1, both operational and physical, that will always be in place;

.5 Detail the additional security measures that will allow the ship to progress without delay to security level 2 and, when necessary, to security level 3;

.6 Provide for regular review, or audit, of the SSP and for its amendment in response to experience or changing circumstances; and

.7 Reporting procedures to the appropriate Contracting Governments contact points.

9.3 Preparation of an effective SSP should rest on a thorough assessment of all issues that relate to the security of the ship, including, in particular, a thorough appreciation of the physical and operational characteristics, including the voyage pattern, of the individual ship.

9.4 All SSPs should be approved by, or on behalf of, the Administration. If an Administration uses a Recognised Security Organisation (RSO) to review or approve the SSP the RSO should not be associated with any other RSO that prepared, or assisted in the preparation of, the plan.

9.5 CSOs and Ship Security Officers (SSOs) should develop procedures to:

.1 Assess the continuing effectiveness of the SSP; and

.2 Prepare amendments of the plan subsequent to its approval.

9.6 The security measures included in the SSP should be in place when the initial verification for compliance with the requirements of chapter XI-2 and Part A of this Code will be carried out. Otherwise the process of issue to the ship of the required International Ship Security Certificate cannot be carried out.

If there is any subsequent failure of security equipment or systems, or suspension of a security measure for whatever reason, equivalent temporary security measures should be adopted, notified to, and agreed by, the Administration.

Organization and Performance of Ship Security Duties

9.7 In addition to the guidance given in section 9.2, the SSP should establish the following which relate to all security levels:

.1 The duties and responsibilities of all shipboard personnel with a security role;

.2 The procedures or safeguards necessary to allow such continuous communications to be maintained at all times;

.3 The procedures needed to assess the continuing effectiveness of security procedures and any security and surveillance equipment and systems, including procedures for identifying and responding to equipment or systems failure or malfunction;

.4 The procedures and practices to protect security sensitive information held in paper or electronic format;

.5 The type and maintenance requirements, of security and surveillance equipment and systems, if any;

.6 The procedures to ensure the timely submission, and assessment, of reports relating to possible breaches of security or security concerns; and

.7 Procedures to establish, maintain and up-date an inventory of any dangerous goods or hazardous substances carried on board, including their location.

9.8 The remainder of this section addresses specifically the security measures that could be taken at each security level covering:

.1 Access to the Ship by ship's personnel, passengers, visitors, etc;

.2 Restricted Areas on the Ship;

.3 Handling of Cargo;

.4 Delivery of Ship's Stores;

.5 Handling Unaccompanied Baggage; and

.6 Monitoring the Security of the Ship.

Access to the Ship

9.9 The SSP should establish the security measures covering all means of access to the ship identified in the SSA. This should include any:

.1 Access ladders;

.2 Access gangways;

.3 Access ramps;

.4 Access doors, side scuttles, windows and ports;

.5 Mooring lines and anchor chains; and

.6 Cranes and hoisting gear.

9.10 For each of these the SSP should identify the appropriate locations where access restrictions or prohibitions should be applied for each of the security levels. For each security level the SSP should establish the type of restriction or prohibition to be applied and the means of enforcing them.

9.11 The SSP should establish for each security level the means of identification required to allow access to the ship and for individuals to remain on the ship without challenge, this may involve developing an appropriate identification system allowing for permanent and temporary identifications, for ship's personnel and visitors respectively.

Any ship identification system should, when it is practicable to do so, be co-ordinated with that applying to the port facility.

Passengers should be able to prove their identity by boarding passes, tickets, etc., but

should not be permitted access to restricted areas unless supervised.

The SSP should establish provisions to ensure that the identification systems are regularly updated, and that abuse of procedures should be subject to disciplinary action.

9.12 Those unwilling or unable to establish their identity and/or to confirm the purpose of their visit when requested to do so should be denied access to the ship and their attempt to obtain access should be reported, as appropriate, to the SSOs, the CSOs, the Port Facility Security Officer (PFSO) and to the national or local authorities with security responsibilities.

9.13 The SSP should establish the frequency of application of any access controls particularly if they are to be applied on a random, or occasional, basis.

Security Level 1

9.14 At security level 1, the SSP should establish the security measures to control access to the ship, where the following may be applied:

- .1 Checking the identity of all persons seeking to board the ship and confirming their reasons for doing so by checking, for example, joining instructions, passenger tickets, boarding passes, work orders etc;
- .2 In liaison with the port facility the ship should ensure that designated secure areas are established in which inspections and searching of people, baggage (including carry on items), personal effects, vehicles and their contents can take place;
- .3 In liaison with the port facility the ship should ensure that vehicles destined to be loaded on board car carriers, ro-ro and other passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP;
- .4 Segregating checked persons and their personal effects from unchecked persons and their personal effects;
- .5 Segregating embarking from disembarking passengers;
- .6 Identification of access points that should be secured or attended to prevent unauthorized access;
- .7 Securing, by locking or other means, access to unattended spaces adjoining areas to which passengers and visitors have access; and
- .8 Providing security briefings to all ship personnel on possible threats, the procedures for reporting suspicious persons, objects or activities and the need for vigilance.

9.15 At security level 1, all those seeking to board a ship should be liable to search. The frequency of such searches, including random searches, should be specified in the approved SSP and should be specifically approved by the Administration. Such searches may best be undertaken by the port facility in close co-operation with the ship and in close proximity to it.

Unless there are clear security grounds for doing so, members of the ship's personnel should not be required to search their colleagues or their personal effects.

Any such search shall be undertaken in a manner which fully takes into account the human rights of the individual and preserves their basic human dignity.

Security Level 2

9.16 At security level 2, the SSP should establish the security measures to be applied to protect against a heightened risk of a security incident to ensure higher vigilance and tighter control, which may include:

- .1 Assigning additional personnel to patrol deck areas during silent hours to deter unauthorized access;
- .2 Limiting the number of access points to the ship, identifying those to be closed and the means of adequately securing them;
- .3 Deterring waterside access to the ship, including, for example, in liaison with the port facility, provision of boat patrols;
- .4 Establishing a restricted area on the shore-side of the ship, in close co-operation with the port facility;
- .5 Increasing the frequency and detail of searches of people, personal effects, and vehicles being embarked or loaded onto the ship;
- .6 Escorting visitors on the ship;
- .7 Providing additional specific security briefings to all ship personnel on any identified threats, re-emphasising the procedures for reporting suspicious persons, objects, or activities and the stressing the need for increased vigilance; and
- .8 Carrying out a full or partial search of the ship.

Security Level 3

9.17 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

- .1 Limiting access to a single, controlled, access point;
- .2 Granting access only to those responding to the security incident or threat thereof;
- .3 Directions of persons on board;
- .4 Suspension of embarkation or disembarkation;
- .5 Suspension of cargo handling operations, deliveries etc;
- .6 Evacuation of the ship;
- .7 Movement of the ship; and
- .8 Preparing for a full or partial search of the ship.

Restricted Areas on the Ship

9.18 The SSP should identify the restricted areas to be established on the ship, specify their extent, times of application, the security measures to be taken to control access to them and those to be taken to control activities within them. The purpose of restricted areas are to:

- .1 Prevent unauthorised access;
- .2 Protect passengers, ship's personnel, and personnel from port facilities or other agencies authorised to be on board the ship;
- .3 Protect sensitive security areas within the ship; and
- .4 Protect cargo and ship's stores from tampering.

9.19 The SSP should ensure that there are clearly established policies and practices to control access to all restricted areas them.

9.20 The SSP should provide that all restricted areas should be clearly marked indicating that access to the area is restricted

and that unauthorised presence within the area constitutes a breach of security.

9.21 Restricted areas may include:

- .1 Navigation bridge, machinery spaces of category A and other control stations as defined in chapter II-2;
- .2 Spaces containing security and surveillance equipment and systems and their controls and lighting system controls;
- .3 Ventilation and air-conditioning systems and other similar spaces;
- .4 Spaces with access to potable water tanks, pumps, or manifolds;
- .5 Spaces containing dangerous goods or hazardous substances;
- .6 Spaces containing cargo pumps and their controls;
- .7 Cargo spaces and spaces containing ship's stores;
- .8 Crew accommodation; and
- .9 Any other areas as determined by the CSO, through the SSA to which access must be restricted to maintain the security of the ship.

Security Level 1

9.22 At security level 1, the SSP should establish the security measures to be applied to restricted areas, which may include:

- .1 Locking or securing access points;
- .2 Using surveillance equipment to monitor the areas;
- .3 Using guards or patrols; and
- .4 Using automatic intrusion detection devices to alert the ship's personnel of unauthorized access.

Security Level 2

9.23 At security level 2, the frequency and intensity of the monitoring of, and control of access to restricted areas should be increased to ensure that only authorized persons have access. The SSP should establish the additional security measures to be applied, which may include:

- .1 Establishing restricted areas adjacent to access points;
- .2 Continuously monitoring surveillance equipment; and
- .3 Dedicating additional personnel to guard and patrol restricted areas.

Security Level 3

9.24 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operations with those responding and the port facility, which may include:

- .1 Setting up of additional restricted areas on the ship in proximity to the security incident, or the believed location of the security threat, to which access is denied; and
- .2 Searching of restricted areas as part of a search of the ship.

Handling of Cargo

9.25 The security measures relating to cargo handling should:

- .1 Prevent tampering, and
- .2 Prevent cargo that is not meant for carriage from being accepted and stored on board the ship.

9.26 The security measures, some of which may have to be applied in liaison with the port facility, should include inventory

control procedures at access points to the ship. Once on board the ship, cargo should be capable of being identified as having been approved for loading onto the ship. In addition, security measures should be developed to ensure that cargo, once on board, is not tampered with.

Security Level 1

9.27 At security level 1, the SSP should establish the security measures to be applied during cargo handling, which may include:

- .1 Routine checking of cargo, cargo transport units and cargo spaces prior to, and during, cargo handling operations;
- .2 Checks to ensure that cargo being loaded matches the cargo documentation;
- .3 Ensuring, in liaison with the port facility, that vehicles to be loaded on board car-carriers, ro-ro and passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP; and

.4 Checking of seals or other methods used to prevent tampering.

9.28 Checking of cargo may be accomplished by the following means:

- .1 Visual and physical examination; and
- .2 Using scanning/detection equipment, mechanical devices, or dogs.

9.29 When there are regular, or repeated, cargo movement the CSO or SSO may, in consultation with the port facility, agree arrangements with shippers or others responsible for such cargo covering off-site checking, sealing, scheduling, supporting documentation, etc. Such arrangements should be communicated to and agreed with the PFSO concerned.

Security Level 2

9.30 At security level 2, the SSP should establish the additional security measures to be applied during cargo handling, which may include:

- .1 Detailed checking of cargo, cargo transport units and cargo spaces;
- .2 Intensified checks to ensure that only the intended cargo is loaded;
- .3 Intensified searching of vehicles to be loaded on car-carriers, ro-ro and passenger ships; and
- .4 Increased frequency and detail in checking of seals or other methods used to prevent tampering.

9.31 Detailed checking of cargo may be accomplished by the following means:

- .1 Increasing the frequency and detail of visual and physical examination;
- .2 Increasing the frequency of the use of scanning/detection equipment, mechanical devices, or dogs; and
- .3 Co-ordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures.

Security Level 3

9.32 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

- .1 Suspension of the loading or unloading of cargo; and

.2 Verify the inventory of dangerous goods and hazardous substances carried on board, if any, and their location.

Delivery of Ship's Stores

9.33 The security measures relating to the delivery of ship's stores should:

- .1 Ensure checking of ship's stores and package integrity;
- .2 Prevent ship's stores from being accepted without inspection;
- .3 Prevent tampering; and
- .4 Prevent ship's stores from being accepted unless ordered.

9.34 For ships regularly using the port facility it may be appropriate to establish procedures involving the ship, its suppliers and the port facility covering notification and timing of deliveries and their documentation. There should always be some way of confirming that stores presented for delivery are accompanied by evidence that they have been ordered by the ship.

Security Level 1

9.35 At security level 1, the SSP should establish the security measures to be applied during delivery of ship's stores, which may include:

- .1 Checking to ensure stores match the order prior to being loaded on board; and
- .2 Ensuring immediate secure stowage of ship's stores.

Security Level 2

9.36 At security level 2, the SSP should establish the additional security measures to be applied during delivery of ship's stores by exercising checks prior to receiving stores on board and intensifying inspections.

Security Level 3

9.37 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

- .1 Subjecting ship's stores to more extensive checking;
- .2 Preparation for restriction or suspension of handling of ship's stores; and
- .3 Refusal to accept ship's stores on board the ship.

Handling Unaccompanied Baggage

9.38 The SSP should establish the security measures to be applied to ensure that unaccompanied baggage (*i.e.* any baggage, including personal effects, which is not with the passenger or member of ship's personnel at the point of inspection or search) is identified and subjected to appropriate screening, including searching, before it is accepted on board the ship.

It is not envisaged that such baggage will be subjected to screening by both the ship and the port facility, and in cases where both are suitably equipped, the responsibility for screening should rest with the port facility.

Close co-operation with the port facility is essential and steps should be taken to ensure that unaccompanied baggage is handled securely after screening.

Security Level 1

9.39 At security level 1, the SSP should establish the security measures to be applied

when handling unaccompanied baggage to ensure that unaccompanied baggage is screened or searched up to and including 100 percent, which may include use of x-ray screening.

Security Level 2

9.40 At security level 2, the SSP should establish the additional security measures to be applied when handling unaccompanied baggage which should include 100 percent x-ray screening of all unaccompanied baggage.

Security Level 3

9.41 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

- .1 Subjecting such baggage to more extensive screening, for example x-raying it from at least two different angles;
- .2 Preparation for restriction or suspension of handling of unaccompanied baggage; and
- .3 Refusal to accept unaccompanied baggage on board the ship.

Monitoring the Security of the Ship

9.42 The ship should have the capability to monitor the ship, the restricted areas on board and areas surrounding the ship. Such monitoring capabilities may include use of:

- .1 Lighting;
- .2 Watch-keepers, security guards and deck watches including patrols, and
- .3 Automatic intrusion detection devices and surveillance equipment.

9.43 When used, automatic intrusion detection devices should activate an audible and/or visual alarm at a location that is continuously attended or monitored.

9.44 The SSP should establish the procedures and equipment needed at each security level and the means of ensuring that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather conditions or of power disruptions.

Security Level 1

9.45 At security level 1, the SSP should establish the security measures to be applied which may be a combination of lighting, watch keepers, security guards or use of security and surveillance equipment to allow ship's security personnel to observe the ship in general, and barriers and restricted areas in particular.

9.46 The ship's deck and access points to the ship should be illuminated during hours of darkness and periods of low visibility while conducting ship/port interface activities or at a port facility or anchorage when necessary.

While underway, when necessary, ships should use the maximum lighting available consistent with safe navigation, having regard to the provisions of the International Regulation for the Prevention of Collisions at Sea in force.

The following should be considered when establishing the appropriate level and location of lighting:

.1 The ship's personnel should be able to detect activities beyond the ship, on both the shore side and the waterside;

.2 Coverage should include the area on and around the ship;

.3 Coverage should facilitate personnel identification at access points; and

.4 Coverage may be provided through coordination with the port facility.

Security Level 2

9.47 At security level 2, the SSP should establish the additional security measures to be applied to enhance the monitoring and surveillance capabilities, which may include:

.1 Increasing the frequency and detail of security patrols;

.2 Increasing the coverage and intensity of lighting or the use of security and surveillance and equipment;

.3 Assigning additional personnel as security lookouts; and

.4 Ensuring coordination with waterside boat patrols, and foot or vehicle patrols on the shore-side, when provided.

9.48 Additional lighting may be necessary to protect against a heightened risk of a security incidents. When necessary, the additional lighting requirements may be accomplished by coordinating with the port facility to provide additional shore side lighting.

Security Level 3

9.49 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.1 Switching on of all lighting on, or illuminating the vicinity of, the ship;

.2 Switching on of all on board surveillance equipment capable of recording activities on, or in the vicinity of, the ship;

.3 Maximising the length of time such surveillance equipment can continue to record;

.4 Preparation for underwater inspection of the hull of the ship; and

.5 Initiation of measures, including the slow revolution of the ship's propellers, if practicable, to deter underwater access to the hull of the ship.

Differing Security Levels

9.50 The SSP should establish details of the procedures and security measures the ship could adopt if the ship is at a higher security level than that applying to a port facility.

Activities Not Covered by the Code

9.51 The SSP should establish details of the procedures and security measures the ship should apply when:

.1 It is at a port of a State which is not a Contracting Government;

.2 It is interfacing with a ship to which this Code does not apply⁷;

.3 It is interfacing with fixed or floating platforms or a mobile drilling unit on location; or

.4 It is interfacing with a port or port facility which is not required to comply with chapter XI-2 and part A of this Code.

Declarations of Security

9.52 The SSP should detail how requests for DoS from a port facility will be handled and the circumstances under which the ship itself should request a DoS.

Audit and Review

9.53 The SSP should establish how the CSO and the SSO intend to audit the continued effectiveness of the SSP and the procedure to be followed to review, update or amend the SSP.

10 Records

10.1 Records should be available to duly authorized officers of Contracting Governments to verify that the provisions of ship security plans are being implemented.

10.2 Records may be kept in any format but should be protected from unauthorized access or disclosure.

11 Company Security Officer

Relevant guidance is provided under sections 8, 9 and 13.

12 Ship Security Officer

Relevant guidance is provided under sections 8, 9 and 13.

13 Training, Drills and Exercises on Ship Security

13.1 The Company Security Officer (CSO) and appropriate shore based Company personnel, and the Ship Security Officer (SSO), should have knowledge of, and receive training, in some or all of the following, as appropriate:

.1 Security administration;

.2 Relevant international conventions, codes and recommendations;

.3 Relevant Government legislation and regulations;

.4 Responsibilities and functions of other security organisations;

.5 Methodology of ship security assessment;

.6 Methods of ship security surveys and inspections;

.7 Ship and port operations and conditions;

.8 Ship and port facility security measures;

.9 Emergency preparedness and response and contingency planning;

.10 Instruction techniques for security training and education, including security measures and procedures;

.11 Handling sensitive security related information and security related communications;

.12 Knowledge of current security threats and patterns;

.13 Recognition and detection of weapons, dangerous substances and devices;

.14 Recognition, on a non discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

.15 Techniques used to circumvent security measures;

.16 Security equipment and systems and their operational limitations;

.17 Methods of conducting audits, inspection, control and monitoring;

.18 Methods of physical searches and non-intrusive inspections;

.19 Security drills and exercises, including drills and exercises with port facilities; and

.20 Assessment of security drills and exercises.

13.2 In addition the SSO should have adequate knowledge of, and receive training, in some or all of the following, as appropriate:

.1 The layout of the ship;

.2 The ship security plan and related procedures (including scenario-based training on how to respond);

.3 Crowd management and control techniques;

.4 Operations of security equipment and systems; and

.5 Testing, calibration and whilst at sea maintenance of security equipment and systems.

13.3 Shipboard personnel having specific security duties should have sufficient knowledge and ability to perform their assigned duties, including, as appropriate:

.1 Knowledge of current security threats and patterns;

.2 Recognition and detection of weapons, dangerous substances and devices;

.3 Recognition of characteristics and behavioural patterns of persons who are likely to threaten security;

.4 Techniques used to circumvent security measures;

.5 Crowd management and control techniques;

.6 Security related communications;

.7 Knowledge of the emergency procedures and contingency plans;

.8 Operations of security equipment and systems;

.9 Testing, calibration and whilst at sea maintenance of security equipment and systems;

.10 Inspection, control, and monitoring techniques; and

.11 Methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores.

13.4 All other shipboard personnel should have sufficient knowledge of and be familiar with relevant provisions of the SSP, including:

.1 The meaning and the consequential requirements of the different security levels;

.2 Knowledge of the emergency procedures and contingency plans;

.3 Recognition and detection of weapons, dangerous substances and devices;

.4 Recognition, on a non discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security; and

.5 Techniques used to circumvent security measures.

13.5 The objective of drills and exercises is to ensure that shipboard personnel are proficient in all assigned security duties at all security levels and the identification of any security related deficiencies, which need to be addressed.

⁷ Refer to Further Work by the International Maritime Organization pertaining to Enhancement of Maritime Security, adopted by the Conference on Maritime Security by resolution 3.

13.6 To ensure the effective implementation of the provisions of the ship security plan, drills should be conducted at least once every three months. In addition, in cases where more than 25 percent of the ship's personnel has been changed, at any one time, with personnel that has not previously participated in any drill on that ship, within the last 3 months, a drill should be conducted within one week of the change. These drills should test individual elements of the plan such as those security threats listed in paragraph 8.9.

13.7 Various types of exercises which may include participation of company security officers, port facility security officers, relevant authorities of Contracting Governments as well as ship security officers, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises. These exercises should test communications, coordination, resource availability, and response. These exercises may be:

- .1 Full scale or live;
- .2 Tabletop simulation or seminar; or
- .3 Combined with other exercises held

such as search and rescue or emergency response exercises.

13.8 Company participation in an exercise with another Contracting Government should be recognised by the Administration.

14 Port Facility Security

Relevant guidance is provided under section 15, 16 and 18.

15 Port Facility Security Assessment

General

15.1 The Port Facility Security Assessment (PFSA) may be conducted by a Recognized Security Organization (RSO).

However, approval of a completed PFSA should only be given by the relevant Contracting Government.

15.2 If a Contracting Government uses a RSO, to review or verify compliance of the PFSA, the RSO should not be associated with any other RSO that prepared or assisted in the preparation of that assessment.

15.3 A PFSA should address the following elements within a port facility:

- .1 Physical security;
- .2 Structural integrity;
- .3 Personnel protection systems;
- .4 Procedural policies;
- .5 Radio and telecommunication systems, including computer systems and networks;
- .6 Relevant transportation infrastructure;
- .7 Utilities; and
- .8 Other areas that may, if damaged or used for illicit observation, pose a risk to people, property, or operations within the port facility.

15.4 Those involved in a PFSA should be able to draw upon expert assistance in relation to:

- .1 Knowledge of current security threats and patterns;
- .2 Recognition and detection of weapons, dangerous substances and devices;
- .3 Recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

.4 Techniques used to circumvent security measures;

.5 Methods used to cause a security incident;

.6 Effects of explosives on structures and port facility services;

.7 Port facility security;

.8 Port business practices;

.9 Contingency planning, emergency preparedness and response;

.10 Physical security measures *e.g.* fences;

.11 Radio and telecommunications systems, including computer systems and networks;

.12 Transport and civil engineering; and

.13 Ship and port operations.

Identification and evaluation of important assets and infrastructure it is important to protect.

15.5 The identification and evaluation of important assets and infrastructure is a process through which the relative importance of structures and installations to the functioning of the port facility can be established.

This identification and evaluation process is important because it provides a basis for focusing mitigation strategies on those assets and structures which it is more important to protect from a security incident.

This process should take into account potential loss of life, the economic significance of the port, symbolic value, and the presence of Government installations.

15.6 Identification and evaluation of assets and infrastructure should be used to prioritise their relative importance for protection.

The primary concern should be avoidance of death or injury. It is also important to consider whether the port facility, structure or installation can continue to function without the asset, and the extent to which rapid re-establishment of normal functioning is possible.

15.7 Assets and infrastructure that should be considered important to protect may include:

- .1 Accesses, entrances, approaches, and anchorages, manoeuvring and berthing areas;
- .2 Cargo facilities, terminals, storage areas, and cargo handling equipment;
- .3 Systems such as electrical distribution systems, radio and telecommunication systems and computer systems and networks;
- .4 Port vessel traffic management systems and aids to navigation;
- .5 Power plants, cargo transfer piping, and water supplies;
- .6 Bridges, railways, roads;
- .7 Port service vessels, including pilot boats, tugs, lighters etc;
- .8 Security and surveillance equipment and systems; and
- .9 The waters adjacent to the port facility.

15.8 The clear identification of assets and infrastructure is essential to the evaluation of the port facility's security requirements, the prioritisation of protective measures, and decisions concerning the allocation of resources to better protect the port facility.

The process may involve consultation with the relevant authorities relating to structures adjacent to the port facility which could cause damage within the facility or be used

for the purpose of causing damage to the facility or for illicit observation of the facility or for diverting attention.

Identification of the possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures.

15.9 Possible acts that could threaten the security of assets and infrastructure, and the methods of carrying out those acts, should be identified to evaluate the vulnerability of a given asset or location to a security incident, and to establish and prioritise security requirements to enable planning and resource allocations.

Identification and evaluation of each potential act and its method should be based on various factors, including threat assessments by Government agencies.

By identifying and assessing threats those conducting the assessment do not have to rely on worst-case scenarios to guide planning and resource allocations.

15.10 The PFSA should include an assessment undertaken in consultation with the relevant national security organizations to determine:

.1 Any particular aspects of the port facility, including the vessel traffic using the facility, which make it likely to be the target of an attack;

.2 The likely consequences in terms of loss of life, damage to property, economic disruption, including disruption to transport systems, of an attack on, or at, the port facility;

.3 The capability and intent of those likely to mount such an attack; and

.4 The possible type, or types, of attack.

Producing an overall assessment of the level of risk against which security measures have to be developed.

15.11 The PFSA should consider all possible threats, which may include the following types of security incidents:

.1 Damage to, or destruction of, the port facility or of the ship, *e.g.* by explosive devices, arson, sabotage or vandalism;

.2 Hijacking or seizure of the ship or of persons on board;

.3 Tampering with cargo, essential ship equipment or systems or ship's stores;

.4 Unauthorised access or use including presence of stowaways;

.5 Smuggling weapons or equipment, including weapons of mass destruction;

.6 Use of the ship to carry those intending to cause a security incident and their equipment;

.7 Use of the ship itself as a weapon or as a means to cause damage or destruction;

.8 Blockage; of port entrances, locks, approaches etc; and

.9 Nuclear, biological and chemical attack.

15.12 The process should involve consultation with the relevant authorities relating to structures adjacent to the port facility which could cause damage within the facility or be used for the purpose of causing damage to the facility or for illicit observation of the facility or for diverting attention.

Identification, selection, and prioritisation of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability.

15.13 The identification and prioritisation of countermeasures is designed to ensure that the most effective security measures are employed to reduce the vulnerability of a port facility or ship/port interface to the possible threats.

15.14 Security measures should be selected on the basis of factors such as whether they reduce the probability of an attack and should be evaluated using information that includes:

- .1 Security surveys, inspections and audits;
- .2 Consultation with port facility owners and operators, and owners/operators of adjacent structures if appropriate;
- .3 Historical information on security incidents; and
- .4 Operations within the port facility.

Identification of Vulnerabilities

15.15 Identification of vulnerabilities in physical structures, personnel protection systems, processes, or other areas that may lead to a security incident can be used to establish options to eliminate or mitigate those vulnerabilities. For example, an analysis might reveal vulnerabilities in a port facility's security systems or unprotected infrastructure such as water supplies, bridges etc. that could be resolved through physical measures, e.g. permanent barriers, alarms, surveillance equipment etc.

15.16 Identification of vulnerabilities should include consideration of:

- .1 Waterside and shore-side access to the port facility and ships berthing at the facility;
- .2 Structural integrity of the piers, facilities, and associated structures;
- .3 Existing security measures and procedures, including identification systems;
- .4 Existing security measures and procedures relating to port services and utilities;
- .5 Measures to protect radio and telecommunication equipment, port services and utilities, including computer systems and networks;
- .6 Adjacent areas that may be exploited during, or for, an attack;
- .7 Existing agreements with private security companies providing waterside/shore-side security services;
- .8 Any conflicting policies between safety and security measures and procedures;
- .9 Any conflicting port facility and security duty assignments;
- .10 Any enforcement and personnel constraints;
- .11 Any deficiencies identified during training and drills; and
- .12 Any deficiencies identified during daily operation, following incidents or alerts, the report of security concerns, the exercise of control measures, audits etc.

16 Port Facility Security Plan

General

16.1 Preparation of the Port Facility Security Plan (PFSP) is the responsibility of the Port Facility Security Officer (PFSO).

While the PFSO need not necessarily personally undertake all the duties associated with the post the ultimate responsibility for ensuring that they are properly performed remains with the individual PFSO.

16.2 The content of each individual PFSP should vary depending on the particular circumstances of the port facility, or facilities, it covers.

The Port Facility Security (PFSA) will have identified the particular features of the port facility, and of the potential security risks, that have led to the need to appoint a PFSO and to prepare a PFSP.

The preparation of the PFSP will require these features, and other local or national security considerations, to be addressed in the PFSP and for appropriate security measures to be established so as to minimise the likelihood of a breach of security and the consequences of potential risks.

Contracting Governments may prepare advice on the preparation and content of a PFSP.

16.3 All PFSPs should:

- .1 Detail the security organisation of the port facility,
- .2 The organisation's links with other relevant authorities and the necessary communication systems to allow the effective continuous operation of the organisation and its links with others, including ships in port;
- .3 Detail the basic security level 1 measures, both operational and physical, that will be in place;
- .4 Detail the additional security measures that will allow the port facility to progress without delay to security level 2 and, when necessary, to security level 3;
- .5 Provide for regular review, or audit, of the PFSP and for its amendments in response to experience or changing circumstances; and
- .6 Reporting procedures to the appropriate Contracting Governments contact points.

16.4 Preparation of an effective PFSP will rest on a thorough assessment of all issues that relate to the security of the port facility, including, in particular, a thorough appreciation of the physical and operational characteristics of the individual port facility.

16.5 Contracting Government should approve the PFSPs of the port facilities under their jurisdiction.

Contracting Governments should develop procedures to assess the continuing effectiveness of each PFSP and may require amendment of the PFSP prior to its initial approval or subsequent to its approval.

The PFSP should make provision for the retention of records of security incidents and threats, reviews, audits, training, drills and exercises as evidence of compliance with those requirements.

16.6 The security measures included in the PFSP should be in place within a reasonable period of the PFSP's approval and the PFSP should establish when each measure will be in place.

If there is likely to be any delay in their provision this should be discussed with the Contracting Government responsible for approval of the PFSP and satisfactory alternative temporary security measures that provide an equivalent level of security should be agreed to cover any interim period.

16.7 The use of firearms on or near ships and in port facilities may pose particular and significant safety risks, in particular in connection with certain dangerous or hazardous substances and should be considered very carefully.

In the event that a Contracting Government decides that it is necessary to use armed personnel in these areas, that Contracting Government should ensure that these personnel are duly authorised and trained in the use of their weapons and that they are aware of the specific risks to safety that are present in these areas.

If a Contracting Government authorizes the use of firearms they should issue specific safety guidelines on their use.

The PFSP should contain specific guidance on this matter in particular with regard its application to ships carrying dangerous goods or hazardous substances.

Organization and Performance of Port Facility Security Duties

16.8 In addition to the guidance given under section 16.3, the PFSP should establish the following which relate to all security levels:

- .1 The role and structure of the port facility security organisation;
- .2 The duties, responsibilities and training requirements of all port facility personnel with a security role and the performance measures needed to allow their individual effectiveness to be assessed;
- .3 The port facility security organisation's links with other national or local authorities with security responsibilities;
- .4 The communication systems provided to allow effective and continuous communication between port facility security personnel, ships in port and, when appropriate, with national or local authorities with security responsibilities;
- .5 The procedures or safeguards necessary to allow such continuous communications to be maintained at all times;
- .6 The procedures and practices to protect security sensitive information held in paper or electronic format;
- .7 The procedures to assess the continuing effectiveness of security measures, procedures and equipment, including identification of, and response to, equipment failure or malfunction;
- .8 The procedures to allow the submission, and assessment, of reports relating to possible breaches of security or security concerns;
- .9 Procedures relating to cargo handling;
- .10 Procedures covering the delivery of ship's stores;
- .11 The procedures to maintain, and update, records of dangerous goods and hazardous substances and their location within the port facility;
- .12 The means of alerting and obtaining the services of waterside patrols and specialist search teams, including bomb searches and underwater searches;
- .13 The procedures for assisting ship security officers in confirming the identity of those seeking to board the ship when requested; and
- .14 The procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship including representatives of seafarers' welfare and labour organisations.

16.9 The remainder of this section addresses specifically the security measures

that could be taken at each security level covering:

- .1 Access to the Port Facility;
- .2 Restricted Areas within the Port Facility;
- .3 Handling of Cargo;
- .4 Delivery of Ship's Stores;
- .5 Handling Unaccompanied Baggage; and
- .6 Monitoring the Security of the Port Facility.

Access to the Port Facility

16.10 The PFSP should establish the security measures covering all means of access to the port facility identified in the PFSA.

16.11 For each of these the PFSP should identify the appropriate locations where access restrictions or prohibitions should be applied for each of the security levels. For each security level the PFSP should specify the type of restriction or prohibition to be applied and the means of enforcing them.

16.12 The PFSP should establish for each security level the means of identification required to allow access to the port facility and for individuals to remain within the port facility without challenge, this may involve developing an appropriate identification system allowing for permanent and temporary identifications, for port facility personnel and for visitors respectively.

Any port facility identification system should, when it is practicable to do so, be co-ordinated with that applying to ships that regularly use the port facility.

Passengers should be able to prove their identity by boarding passes, tickets, etc., but should not be permitted access to restricted areas unless supervised.

The PFSP should establish provisions to ensure that the identification systems are regularly updated, and that abuse of procedures should be subject to disciplinary action.

16.13 Those unwilling or unable to establish their identity and/or to confirm the purpose of their visit when requested to do so should be denied access to the port facility and their attempt to obtain access should be reported to the PFSP and to the national or local authorities with security responsibilities.

16.14 The PFSP should identify the locations where people, personal effects, and vehicle searches are to be undertaken. Such locations should be covered to facilitate continuous operation regardless of prevailing weather conditions, in accordance with the frequency laid down in the PFSP. Once subjected to search people, personal effects and vehicles should proceed directly to the restricted holding, embarkation or car loading areas.

16.15 The PFSP should establish separate locations for checked and unchecked persons and their effects and if possible separate areas for embarking/disembarking passengers, ship's personnel and their effects to ensure that unchecked persons are not able to come in contact with checked persons.

16.16 The PFSP should establish the frequency of application of any access controls particularly if they are to be applied on a random, or occasional, basis.

Security Level 1

16.17 At security level 1, the PFSP should establish the control points where the following security measures may be applied:

- .1 Restricted areas which should be bound by fencing or other barriers to a standard which should be approved by the Contracting Government;
- .2 Checking identity of all persons seeking entry to the port facility in connection with a ship, including passengers, ship's personnel and visitors and confirming their reasons for doing so by checking, for example, joining instructions, passenger tickets, boarding passes, work orders, etc;
- .3 Checking vehicles used by those seeking entry to the port facility in connection with a ship;
- .4 Verification of the identity of port facility personnel and those employed within the port facility and their vehicles;
- .5 Restricting access to exclude those not employed by the port facility or working within it, if they are unable to establish their identity;
- .6 Undertaking searches of people, personal effects, vehicles and their contents; and
- .7 Identification of any access points not in regular use which should be permanently closed and locked.

16.18 At security level 1, all those seeking access to the port facility should be liable to search. The frequency of such searches, including random searches, should be specified in the approved PFSP and should be specifically approved by the Contracting Government.

Unless there are clear security grounds for doing so, members of the ship's personnel should not be required to search their colleagues or their personal effects.

Any such search shall be undertaken in a manner which fully takes into account the human rights of the individual and preserves their basic human dignity.

Security Level 2

16.19 At security level 2, the PFSP should establish the additional security measures to be applied, which may include:

- .1 Assigning additional personnel to guard access points and patrol perimeter barriers;
- .2 Limiting the number of access points to the port facility, and identify those to be closed and the means of adequately securing them;
- .3 Providing for means of impeding movement through the remaining access points, e.g. security barriers;
- .4 Increasing the frequency of searches of persons, personal effects, and vehicle;
- .5 Deny access to visitors who are unable to provide a verifiable justification for seeking access to the port facility; and
- .6 Using of patrol vessels to enhance waterside security;

Security Level 3

16.20 At security level 3, the port facility should comply with instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with

those responding and the ships at the port facility, which may include:

- .1 Suspension of access to all, or part of, the port facility;
- .2 Granting access only to those responding to the security incident or threat thereof;
- .3 Suspension of pedestrian or vehicular movement within all, or part, of the port facility;
- .4 Increased security patrols within the port facility, if appropriate;
- .5 Suspension of port operations within all, or part, of the port facility;
- .6 Direction of vessel movements relating to all, or part, of the port facility; and
- .7 Evacuation of all, or part of, the port facility.

Restricted Areas Within the Port Facility

16.21 The PFSP should identify the restricted areas to be established within the port facility, specify their extent, times of application, the security measures to be taken to control access to them and those to be taken to control activities within them. This should also include, in appropriate circumstances, measures to ensure that temporary restricted areas are security swept both before and after that area is established.

The purpose of restricted areas is to:

- .1 Protect passengers, ship's personnel, port facility personnel and visitors, including those visiting in connection with a ship;
- .2 Protect the port facility;
- .3 Protect ships using, and serving, the port facility;
- .4 Protect sensitive security locations and areas within the port facility,
- .5 To protect security and surveillance equipment and systems; and
- .6 Protect cargo and ship's stores from tampering.

16.22 The PFSP should ensure that all restricted areas have clearly established security measures to control:

- .1 Access by individuals;
- .2 The entry, parking, loading and unloading of vehicles;
- .3 Movement and storage of cargo and ship's stores, and
- .4 Unaccompanied baggage or personal effects.

16.23 The PFSP should provide that all restricted areas should be clearly marked indicating that access to the area is restricted and that unauthorised presence within the area constitutes a breach of security.

16.24 When automatic intrusion detection devices are installed they should alert a control centre which can respond to the triggering of an alarm.

16.25 Restricted areas may include:

- .1 Shore and waterside areas immediately adjacent to the ship;
- .2 Embarkation and disembarkation areas, passenger and ship's personnel holding and processing areas including search points;
- .3 Areas where loading, unloading or storage of cargo and stores is undertaken;
- .4 Locations where security sensitive information, including cargo documentation, is held;
- .5 Areas where dangerous goods and hazardous substances are held;
- .6 Vessel traffic management system control rooms, aids to navigation and port

control buildings, including security and surveillance control rooms;

.7 Areas where security and surveillance equipment are stored or located;

.8 Essential electrical, radio and telecommunication, water and other utility installations; and

.9 Other locations in the port facility where access by vessels, vehicles and individuals should be restricted.

16.26 The security measures may extend, with the agreement of the relevant authorities, to restrictions on unauthorised access to structures from which the port facility can be observed.

Security Level 1

16.27 At security level 1, the PFSP should establish the security measures to be applied to restricted areas, which may include:

.1 Provision of permanent or temporary barriers to surround the restricted area whose standard should be accepted by the Contracting Government;

.2 Provision of access points where access can be controlled by security guards when in operation and which can be effectively locked or barred when not in use;

.3 Providing passes which must be displayed to identify individuals entitlement to be within the restricted area;

.4 Clearly marking vehicles allowed access to restricted areas;

.5 Providing guards and patrols;

.6 Providing automatic intrusion detection devices, or surveillance equipment or systems to detect unauthorised access into, or movement within restricted areas; and

.7 Control of the movement of vessels in the vicinity of ships using the port facility.

Security Level 2

16.28 At security level 2, the PFSP should establish the enhancement of the frequency and intensity of the monitoring of, and control of access to, restricted areas. The PFSP should establish the additional security measures, which may include:

.1 Enhancing the effectiveness of the barriers or fencing surrounding restricted areas, including the use of patrols or automatic intrusion detection devices;

.2 Reducing the number of access points to restricted areas and enhancing the controls applied at the remaining accesses;

.3 Restrictions on parking adjacent to berthed ships;

.4 Further restricting access to the restricted areas and movements and storage within them;

.5 Use of continuously monitored and recording surveillance equipment;

.6 Enhancing the number and frequency of patrols including waterside patrols undertaken on the boundaries of the restricted areas and within the areas;

.7 Establishing and restricting access to areas adjacent to the restricted areas; and

.8 Enforcing restrictions on access by unauthorised craft to the waters adjacent to ships using the port facility.

Security Level 3

16.29 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident

or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include:

.1 Setting up of additional restricted areas within the port facility in proximity to the security incident, or the believed location of the security threat, to which access is denied; and

.2 Preparing for the searching of restricted areas as part of a search of all, or part, of the port facility.

Handling of Cargo

16.30 The security measures relating to cargo handling should:

.1 Prevent tampering, and

.2 Prevent cargo that is not meant for carriage from being accepted and stored within the port facility.

16.31 The security measures should include inventory control procedures at access points to the port facility. Once within the port facility cargo should be capable of being identified as having been checked and accepted for loading onto a ship or for temporary storage in a restricted area while awaiting loading. It may be appropriate to restrict the entry of cargo to the port facility that does not have a confirmed date for loading.

Security Level 1

16.32 At security level 1, the PFSP should establish the security measures to be applied during cargo handling, which may include:

.1 Routine checking of cargo, cargo transport units and cargo storage areas within the port facility prior to, and during, cargo handling operations;

.2 Checks to ensure that cargo entering the port facility matches the delivery note or equivalent cargo documentation;

.3 Searches of vehicles; and

.4 Checking of seals and other methods used to prevent tampering upon entering the port facility and upon storage within the port facility.

16.33 Checking of cargo may be accomplished by some or all of the following means:

.1 Visual and physical examination; and

.2 Using scanning/detection equipment, mechanical devices, or dogs.

16.34 When there are regular, or repeated, cargo movement the Company Security Officer (CSO) or the Ship Security Officer (SSO) may, in consultation with the port facility, agree arrangements with shippers or others responsible for such cargo covering off-site checking, sealing, scheduling, supporting documentation, etc. Such arrangements should be communicated to and agreed with the PFSP concern.

Security Level 2

16.35 At security level 2, the PFSP should establish the additional security measures to be applied during cargo handling to enhance control, which may include:

.1 Detailed checking of cargo, cargo transport units and cargo storage areas within the port facility;

.2 Intensified checks, as appropriate, to ensure that only the documented cargo enters

the port facility, is temporarily stored there and then loaded onto the ship;

.3 Intensified searches of vehicles; and

.4 Increased frequency and detail in checking of seals and other methods used to prevent tampering.

16.36 Detailed checking of cargo may be accomplished by some or all of the following means:

.1 Increasing the frequency and detail of checking of cargo, cargo transport units and cargo storage areas within the port facility (visual and physical examination);

.2 Increasing the frequency of the use of scanning/detection equipment, mechanical devices, or dogs; and

.3 Co-ordinating enhanced security measures with the shipper or other responsible party in addition to an established agreement and procedures.

Security Level 3

16.37 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include:

.1 Restriction or suspension of cargo movements or operations within all, or part, of the port facility or specific ships; and

.2 Verifying the inventory of dangerous goods and hazardous substances held within the port facility and their location.

Delivery of Ship's Stores

16.38 The security measures relating to the delivery of ship's stores should:

.1 Ensure checking of ship's stores and package integrity;

.2 Prevent ship's stores from being accepted without inspection;

.3 Prevent tampering;

.4 Prevent ship's stores from being accepted unless ordered;

.5 Ensure searching the delivery vehicle; and

.6 Ensure escorting delivery vehicles within the port facility.

16.39 For ships regularly using the port facility it may be appropriate to establish procedures involving the ship, its suppliers and the port facility covering notification and timing of deliveries and their documentation. There should always be some way of confirming that stores presented for delivery are accompanied by evidence that they have been ordered by the ship.

Security Level 1

16.40 At security level 1, the PFSP should establish the security measures to be applied to control the delivery of ship's stores, which may include:

.1 Checking of ship's stores;

.2 Advance notification as to composition of load, driver details and vehicle registration; and

.3 Searching the delivery vehicle.

16.41 Checking of ship's stores may be accomplished by some or all of the following means:

.1 Visual and physical examination; and

.2 Using scanning/detection equipment, mechanical devices or dogs.

Security Level 2

16.42 At security level 2, the PFSP should establish the additional security measures to be applied to enhance the control of the delivery of ship's stores, which may include:

- .1 Detailed checking of ship's stores;
- .2 Detailed searches of the delivery vehicles;
- .3 Co-ordination with ship personnel to check the order against the delivery note prior to entry to the port facility; and
- .4 Escorting the delivery vehicle within the port facility.

16.43 Detailed checking of ship's stores may be accomplished by some or all of the following means:

- .1 Increasing the frequency and detail of searches of delivery vehicles;
- .2 Increasing the use of scanning/detection equipment, mechanical devices, or dogs; and
- .3 Restricting, or prohibiting, entry of stores that will not leave the port facility within a specified period.

Security Level 3

16.44 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility which may include preparation for restriction, or suspension, of the delivery of ship's stores within all, or part, of the port facility.

Handling Unaccompanied Baggage

16.45 The PFSP should establish the security measures to be applied to ensure that unaccompanied baggage (*i.e.*, any baggage, including personal effects, which is not with the passenger or member of ship's personnel at the point of inspection or search) is identified and subjected to appropriate screening, including searching, before is allowed in the port facility and, depending on the storage arrangements, before it is transferred between the port facility and the ship.

It is not envisaged that such baggage will be subjected to screening by both the port facility and the ship, and in cases where both are suitably equipped, the responsibility for screening should rest with the port facility.

Close co-operation with the ship is essential and steps should be taken to ensure that unaccompanied baggage is handled securely after screening.

Security Level 1

16.46 At security level 1, the PFSP should establish the security measures to be applied when handling unaccompanied baggage to ensure that unaccompanied baggage is screened or searched up to and including 100 percent, which may include use of x-ray screening.

Security Level 2

16.47 At security level 2, the PFSP should establish the additional security measures to be applied when handling unaccompanied baggage which should include 100 percent x-ray screening of all unaccompanied baggage.

Security Level 3

16.48 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include:

- .1 Subjecting such baggage to more extensive screening, for example x-raying it from at least two different angles;
- .2 Preparations for restriction or suspension of handling or unaccompanied baggage; and
- .3 Refusal to accept unaccompanied baggage into the port facility.

Monitoring the Security of the Port Facility

16.49 The port facility security organization should have the capability to monitor the port facility and its nearby approaches, on land and water, at all times, including the night hours and periods of limited visibility, the restricted areas within the port facility, the ships at the port facility and areas surrounding ships. Such monitoring can include use of:

- .1 Lighting;
- .2 Security guards, including foot, vehicle and waterborne patrols, and
- .3 Automatic intrusion detection devices and surveillance equipment.

16.50 When used, automatic intrusion detection devices should activate an audible and/or visual alarm at a location that is continuously attended or monitored.

16.51 The PFSP should establish the procedures and equipment needed at each security level and the means of ensuring that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather or of power disruptions.

Security Level 1

16.52 At security level 1, the PFSP should establish the security measures to be applied which may be a combination of lighting, security guards or use of security and surveillance equipment to allow port facility security personnel to:

- .1 Observe the general port facility area, including shore and water-side accesses to it;
- .2 Observe access points, barriers and restricted areas, and
- .3 Allow port facility security personnel to monitor areas and movements adjacent to ships using the port facility, including augmentation of lighting provided by the ship itself.

Security Level 2

16.53 At security level 2, the PFSP should establish the additional security measures to be applied to enhance the monitoring and surveillance capability, which may include:

- .1 Increasing the coverage and intensity of lighting and surveillance equipment, including the provision of additional lighting and surveillance coverage;
- .2 Increasing the frequency of foot, vehicle or waterborne patrols, and
- .3 Assigning additional security personnel to monitor and patrol.

Security Level 3

16.54 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include:

- .1 Switching on all lighting within, or illuminating the vicinity of, the port facility;
- .2 Switching on all surveillance equipment capable of recording activities within, or adjacent to, the port facility; and
- .3 Maximising the length of time such surveillance equipment can continue to record.

Differing Security Levels

16.55 The PFSP should establish details of the procedures and security measures the port facility could adopt if the port facility is at a lower security level than that applying to a ship.

Activities not covered by the Code

16.56 The PFSP should establish details of the procedures and security measures the port facility should apply when:

- .1 It is interfacing with a ship which has been at a port of a State which not a Contracting Government;
- .2 It is interfacing with a ship to which this Code does not apply; and
- .3 It is interfacing with fixed or floating platforms or mobile offshore drilling units on location.

Declarations of Security

16.57 The PFSP should establish the procedures to be followed when on the instructions of the Contracting Government the PFSO requests a Declaration of Security or when a DoS is requested by a ship.

Audit, Review and Amendment

16.58 The PFSP should establish how the PFSO intends to audit the continued effectiveness of the PFSP and the procedure to be followed to review, update or amend the PFSP.

16.59 The PFSP should be reviewed at the discretion of the PFSO. In addition it should be reviewed:

- .1 If the PFSA relating to the port facility is altered;
- .2 If an independent audit of the PFSP or the Contracting Government's testing of the port facility security organization identifies failings in the organization or questions the continuing relevance of significant element of the approved PFSP;
- .3 Following security incidents or threats thereof involving the port facility; and
- .4 Following changes in ownership or operational control of the port facility.

16.60 The PFSO can recommend appropriate amendments to the approved plan following any review of the plan. Amendments to the PFSP relating to:

- .1 Proposed changes which could fundamentally alter the approach adopted to maintaining the security of the port facility; and
- .2 The removal, alteration or replacement of permanent barriers, security and surveillance equipment and systems etc.,

previously considered essential in maintaining the security of the port facility; Should be submitted to the Contracting Government that approved the original PFSP for their consideration and approval. Such approval can be given by, or on behalf of, the Contracting Government with, or without, amendments to the proposed changes.

On approval of the PFSP the Contracting Government should indicate which procedural or physical alterations have to be submitted to it for approval.

Approval of Port Facility Security Plans

16.61 PFSPs have to be approved by the relevant Contracting Government which should establish appropriate procedures to provide for:

- .1 The submission of PFSPs to them;
- .2 The consideration of PFSPs;
- .3 The approval of PFSPs, with or without amendments;
- .4 Consideration of amendments submitted after approval, and
- .5 Procedures for inspecting or auditing the continuing relevance of the approved PFSP.

At all stages steps should be taken to ensure that the contents of the PFSP remains confidential.

Statement of Compliance of a Port Facility

16.62 The Contracting Government within whose territory a port facility is located may issue an appropriate Statement of Compliance of a Port Facility (SoCPF) indicating:

- .1 The port facility;
- .2 That the port facility complies with the provisions of chapter XI-2 and part A of the Code.
- .3 The period of validity of the SoCPF which should be specified by the Contracting Governments but should not exceed five years; and
- .4 The subsequent verification arrangements established by the Contracting Government and a confirmation when these are carried out.

16.63 The Statement of Compliance for Port Facility should be in form set out in the appendix to this Part of the Code. If the language used is not Spanish, French or English, the Contracting Government, if it considers it appropriate may also include a translation into one of these languages.

17 Port facility security officer

17.1 In those exceptional instances where the ship security officer has questions about the validity of credentials of those seeking to board the ship for official purposes, the port facility security officer should assist.

17.2 The port facility security officer should not be responsible for routine confirmation of the identity of those seeking to board the ship.

In addition relevant guidance is provided under sections 15, 16 and 18.

18 Training, drills and exercises for port facility security

18.1 The Port Facility Security Officer should have knowledge and receive training, in some or all of the following, as appropriate:

- .1 Security administration;
- .2 Relevant international conventions, codes and recommendations;
- .3 Relevant Government legislation and regulations;
- .4 Responsibilities and functions of other security organisations;
- .5 Methodology of port facility security assessment;
- .6 Methods of ship and port facility security surveys and inspections;
- .7 Ship and port operations and conditions;
- .8 Ship and port facility security measures;
- .9 Emergency preparedness and response and contingency planning;
- .10 Instruction techniques for security training and education, including security measures and procedures;
- .11 Handling sensitive security related information and security related communications;
- .12 Knowledge of current security threats and patterns;
- .13 Recognition and detection of weapons, dangerous substances and devices;
- .14 Recognition, on a non discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten the security;
- .15 Techniques used to circumvent security measures;
- .16 Security equipment and systems, and their operational limitations;
- .17 Methods of conducting audits, inspection, control and monitoring;
- .18 Methods of physical searches and non-intrusive inspections;
- .19 Security drills and exercises, including drills and exercises with ships; and
- .20 Assessment of security drills and exercises.

18.2 Port facility personnel having specific security duties should have knowledge and receive training, in some or all of the following, as appropriate:

- .1 Knowledge of current security threats and patterns;
- .2 Recognition and detection of weapons, dangerous substances and devices;
- .3 Recognition of characteristics and behavioural patterns of persons who are likely to threaten security;
- .4 Techniques used to circumvent security measures;
- .5 Crowd management and control techniques;
- .6 Security related communications;
- .7 Operations of security equipment and systems;
- .8 Testing, calibration and maintenance of security equipment and systems;
- .9 Inspection, control, and monitoring techniques; and
- .10 Methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores.

18.3 All other port facility personnel should have knowledge of and be familiar with relevant provisions of the PFSP, in some or all of the following, as appropriate:

- .1 The meaning and the consequential requirements of the different security levels;

- .2 Recognition and detection of weapons, dangerous substances and devices;
- .3 Recognition of characteristics and behavioural patterns of persons who are likely to threaten the security; and
- .4 Techniques used to circumvent security measures.

18.4 The objective of drills and exercises is to ensure that port facility personnel are proficient in all assigned security duties, at all security levels, and to identify any security related deficiencies, which need to be addressed.

18.5 To ensure the effective implementation of the provisions of the port facility security plan, drills should be conducted at least every three months unless the specific circumstances dictate otherwise. These drills should test individual elements of the plan such as those security threats listed in paragraph 15.11.

18.6 Various types of exercises which may include participation of port facility security officers, in conjunction with relevant authorities of Contracting Governments, company security officers, or ship security officers, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises. Requests for the participation of company security officers or ships security officers in joint exercise should be made bearing in mind the security and work implications for the ship. These exercises should test communication, coordination, resource availability and response. These exercises may be:

- .1 Full scale or live;
- .2 Tabletop simulation or seminar; or
- .3 Combined with other exercises held such as emergency response or other port State authority exercises.

19 Verification and certification for ships

No additional guidance.

Appendix to Part B

Appendix 1—Form of a Declaration of Security

Declaration of Security

Name of Ship:

Port of Registry:

IMO Number:

Name of Port Facility:

This Declaration of Security is valid from _____ until _____, for the following activities _____ (list the activities with relevant details) under the following security levels:

Security level(s) for the ship:

Security level(s) for the port facility:

The port facility and ship agree to the following security measures and responsibilities to ensure compliance with the requirements of Part A of the International Code for the Security of Ships and of Port Facilities.

Activity	The port facility	The ship
The affixing of the initials of the SSO or PFSO under these columns indicates that the activity will be done, in accordance with relevant approved plan, by		
Ensuring the performance of all security duties Monitoring restricted areas to ensure that only authorized personnel have access Controlling access to the port facility Controlling access to the ship Monitoring of the port facility, including berthing areas and areas surrounding the ship Monitoring of the ship, including berthing areas and areas surrounding the ship Handling of cargo Delivery of ship's stores Handling unaccompanied baggage Controlling the embarkation of persons and their effects Ensuring that security communication is readily available between the ship and port facility		

The signatories to this agreement certify that security measures and arrangements for both the port facility and the ship during the specified activities meet the provisions of chapter XI-2 and Part A of Code that will be implemented in accordance with the provisions already stipulated in their approved plan or the specific arrangements agreed to and set out in the attached annex.

Dated at _____ on the _____.

SIGNED FOR AND ON BEHALF OF

The port facility	the ship
(Signature of Port Facility Security Officer)	(Signature of Master or Ship Security Officer)

NAME AND TITLE OF PERSON WHO SIGNED

Name:	Name:
Title:	Title:

CONTACT DETAILS (TO BE COMPLETED AS APPROPRIATE)

[Indicate the telephone numbers or the radio channels or frequencies to be used]

for the port facility:	for the ship:
Port Facility Port Facility Security Officer	Master Ship Security Officer Company Company Security Officer

Appendix 2—Form of a Statement of Compliance of a Port Facility

Statement of Compliance of a Port Facility

(Official seal)

(State)

Statement Number

Issued under the provisions of part B of the International Code for the Security of Ships and of Port Facilities (ISPS CODE).

The Government of _____ (name of the State).

Name of the Port Facility: _____

Address of the Port Facility : _____

This is to Certify that the compliance of this port facility with the provisions of chapter XI-2 and part A of the International Code for the Security of Ships and of Port Facilities (ISPS Code) has been verified and that this port facility operates in accordance with the approved Port Facility Security Plan. This plan has been approved for the

following <specify the types of operations, types of ship or activities or other relevant information>: (delete as appropriate):

Passenger ship
 Passenger high speed craft
 Cargo high speed craft
 Bulk carrier
 Oil tanker
 Chemical tanker
 Gas carrier
 Mobile offshore Drilling Units
 Cargo ships other than those referred to above

This Statement of Compliance is valid until _____, subject to verifications (as indicated overleaf).
 Issued at _____ (place of issue of the statement)
 Date of issue _____

(Signature of the duly authorized official issuing the document)

(Seal or stamp of issuing authority, as appropriate)

Endorsement for Verifications

The Government of <insert name of the State> has established that the validity of this Document of Compliance is subject to <insert relevant details of the verifications (e.g. mandatory annual or unscheduled)>.

This is to Certify that, during a verification carried out in accordance with paragraph B/16.40.3 of the ISPS Code, the Port Facility was found to comply with the relevant provisions of chapter XI-2 of the Convention and Part A of the ISPS Code.

1st Verification

Signed: _____
(Signature of authorized official)

Place: _____

Date: _____

2nd Verification

Signed: _____
(Signature of authorized official)

Place: _____

Date: _____

3rd Verification

Signed: _____
(Signature of authorized official)

Place: _____

Date: _____

4th Verification

Signed: _____
(Signature of authorized official)

Place: _____

Date: _____

Appendix C**Cost Analysis Report for Vessel, Facility, and Port Security, December 20, 2002, Standards Evaluation and Analysis Division, U.S. Coast Guard Headquarters**

Acronyms

AOR—Area of Responsibility

BLS—U.S. Department of Labor Bureau of Labor Statistics

CCTV—Closed Circuit Television

CFR—Code of Federal Regulations

COTP—Captain of the Port

CSO—Company Security Officer

DOT—U.S. Department of Transportation

FSA—Facility Security Assessment

FSO—Facility Security Officer

FSP—Facility Security Plan

GT—Gross Tons

IMO—International Maritime Organization

ISPS Code—International Code for the Security of Ships and of Port Facilities

ITB—Integrated Tug-Barge

MARAD—U.S. Maritime Administration

MARSEC—Maritime Security Level

MODU—Mobile Offshore Drilling Unit

MSMS—Marine Safety Management System

NAICS—North American Industry Classification System

NVIC—Navigation and Vessel Inspection Circular

O&M—Operation and Maintenance

OSV—Offshore Supply Vessel

PFSA—Port Facility Security Assessment

PFSC—Port Facility Security Committee

PFSP—Port Facility Security Plan

PFSO—Port Facility Security Officer

PSA—Port Security Assessment

PSC—Port Security Committee

PSP—Port Security Plan

PV—Present Value

SBA—Small Business Administration

SOLAS—Convention for the Safety of Life at Sea

VSA—Vessel Security Assessment

VSP—Vessel Security Plan

Contents

Executive Summary

Vessel security

Summary

Analysis

Period of analysis

Population affected

Unit cost assumptions

Vessel costs

Company costs

Total national cost of vessel security

Facility security

Summary

Analysis

Period of analysis

Population affected

Unit cost assumptions

Facility costs

Total national cost for facility security

Port security

Summary

Analysis

Period of analysis

Population affected

Unit cost assumptions

Total national cost for port security

Tables

Table 1. Estimated U.S.-Flagged SOLAS population

Table 2. Estimated domestic population

Table 3. Unit cost of equipment

Table 4. Unit cost of personnel

Table 5. Cost per U.S.-flagged SOLAS freight ship

Table 6. Cost per U.S.-flagged SOLAS freight barge

Table 7. Cost per domestic freight ship

Table 8. Cost per domestic freight barge

Table 9. Cost per U.S.-flagged SOLAS tank ship

Table 10. Cost per U.S.-flagged SOLAS tank barge

Table 11. Cost per domestic tank ship

Table 12. Cost per domestic tank barge

Table 13. Cost per U.S.-flagged SOLAS towboat

Table 14. Cost per U.S.-flagged SOLAS fish processor

Table 15. Cost per domestic towboat

Table 16. Cost per U.S.-flagged SOLAS cruise vessel

Table 17. Cost per other U.S.-flagged SOLAS passenger vessel

Table 18. Cost per domestic passenger vessel, not ferry

Table 19. Cost per domestic ferry > 500 passengers

Table 20. Cost per domestic ferry ≤ 500 passengers

Table 21. Cost per domestic cruise vessel

Table 22. Cost per domestic passenger vessel, not ferry

Table 23. Cost per domestic ferry > 500 passengers

Table 24. Cost per domestic ferry ≤ 500 passengers

Table 25. Cost per U.S.-flagged SOLAS MODU

Table 26. Cost per domestic MODU

Table 27. Cost per U.S.-flagged SOLAS OSV

Table 28. Cost per domestic OSV

Table 29. Cost per U.S.-flagged SOLAS oil recovery vessel

Table 30. Cost per U.S.-flagged SOLAS research vessel

Table 31. Cost per U.S.-flagged SOLAS industrial vessel

Table 32. Cost per company by type

Table 33. Example cost for U.S.-flagged SOLAS company

Table 34. Example cost for large non-towing company (no passenger vessels)

Table 35. Example cost for large non-towing company (with passenger vessels)

Table 36. Example cost for large towing company

Table 37. Example cost for small non-towing company

Table 38. Example cost for small towing company

Table 39. Total national PV cost for vessel security, in \$millions

Table 40. Total national initial and annual cost by element of compliance, in \$millions

Table 41. Estimated facility population

Table 42. Unit cost of equipment

Table 43. Unit cost of personnel

Table 44. Initial and annual cost for a non-specific group A facility

Table 45. Initial and annual cost for a non-specific group B facility

Table 46. Estimated percentage of facilities that will purchase or enhance security measures

Table 47. Initial and annual cost for container or break-bulk facilities, group A

Table 48. Initial and annual cost for container or break-bulk facilities, group B

Table 49. Initial and annual cost for dry bulk facilities, group A

Table 50. Initial and annual cost for dry bulk facilities, group B

Table 51. Initial and annual cost for hazardous bulk liquid facilities, group A

Table 52. Initial and annual cost for hazardous bulk liquid facilities, group B

Table 53. Initial and annual cost for hazardous substance (other) facilities, group A

Table 54. Initial and annual cost for hazardous substance (other) facilities, group B

Table 55. Initial and annual cost for other bulk liquid facilities, group A

Table 56. Initial and annual cost for other bulk liquid facilities, group B

Table 57. Initial and annual cost for ferry terminals, group A

Table 58. Initial and annual cost for ferry terminals, group B

Table 59. Initial and annual cost for passenger terminals, group A

Table 60. Initial and annual cost for passenger terminals, group B

Table 61. Example cost for ferry terminal owner

Table 62. Example cost for dry bulk facility owner

Table 63. Example cost for petroleum facility owner

Table 64. Total national PV cost for facility security, in \$millions

Table 65. Total national initial and annual cost by element of compliance, in \$millions

Table 66. PSC meeting frequency, hours, and unit cost per stakeholder

Table 67. PSP planning and drill frequency, hours, and unit cost per stakeholder

Table 68. Total national PV cost for port security, in \$millions

Executive Summary**Note:** for definition of acronyms, refer to the list at the beginning of the report.

The United States has been a participant in negotiations at IMO developing the ISPS Code. This analysis presents the scope and magnitude of costs that the maritime transportation industry could incur for implementing

and complying with the ISPS Code, parts A and B, and Coast Guard issued NVICs (4-02, 9-02, 10-02). The purpose of this report is to present the broad set of assumptions that we used to develop our cost estimates, document our analysis, and make that information available to the public for comment.

For the purposes of good business practice or regulations promulgated by other Federal and State agencies, many companies have spent, to date, a substantial amount of money and resources to upgrade and improve security. The costs shown in this analysis do not include resources these companies have already spent to enhance security.

We realize that every company engaged in maritime commerce would not implement the ISPS Code exactly as presented in this analysis. Depending on each company's choices, some companies could spend much less than what is estimated herein while others could spend significantly more. In general, we assume that each company would implement the ISPS Code based on the type of vessels or facilities it owns or operates and whether it engages in international or domestic trade.

The ISPS Code provides requirements for "Port Facilities." Because the Coast Guard differentiates between ports and facilities in domestic regulations, however, we are presenting this cost analysis in three sections: vessel security, facility security, and port security. As a result, for the purposes of this cost analysis, the terms PFSC, PFSO, PFSA, and PFSP have been replaced with PSC and PSP for the port security section and FSO, FSA, and FSP for the facility security section.

This analysis presents the estimated cost if vessels, facilities, and ports are operating at MARSEC 1 (the current level of operations since the events of September 11, 2001). We do not estimate costs for MARSEC 2 or 3 because the nature of a threat will determine the cost of responding to that threat. Depending on circumstances, one port, a U.S. coast, or the entire country could have an elevated MARSEC level. The costs for this vast range of threat levels are difficult to estimate with any accuracy. Under MARSEC 2 and 3, we would expect not just the immediate effects of increasing security with more personnel and more screening, but also "ripple" effects—delayed commerce, decreased product availability, price increases, increased unemployment, unstable markets worldwide, even negative psychological effects of threats. The recent shut-down of the West Coast ports, while not in response to a security threat, present a

good example of the economic costs that we could experience under increased MARSEC levels.

We do not anticipate that implementing the ISPS Code will require additional manning aboard vessels; the duties envisioned can be assumed by existing personnel. For facilities, we anticipate additional personnel in the form of security guards that can be hired through contracting with a private firm specializing in security.

Based on this analysis, the first-year cost of implementing the ISPS Code for vessels, facilities, and ports is approximately \$1.4 billion, with costs of approximately PV \$6.0 billion over the next 10 years (2003–2012, 7 percent discount rate). Estimated costs are as follows.

- **Vessel Security**—The first-year cost of purchasing equipment, hiring security officers, and preparing paperwork is approximately \$188 million. Following initial implementation, the annual cost is approximately \$144 million. Over the next 10 years, the cost would be PV \$1.1 billion approximately. The paperwork burden associated with planning would be approximately 141,000 hours in the first year and 7,000 hours in subsequent years.

- **Facility Security**—The first-year cost of purchasing equipment, hiring security officers, and preparing paperwork is an estimated \$963 million. Following initial implementation, the annual cost is approximately \$535 million. Over the next 10 years, the cost would be PV \$4.4 billion approximately. The paperwork burden associated with planning would be approximately 464,000 hours in the first year and 17,000 hours in subsequent years.

- **Port Security**—The first-year cost is approximately \$120 million. The second-year cost is approximately \$106 million. In subsequent years, the annual cost is approximately \$46 million. Over the next 10 years, the cost would be PV \$477 million approximately. The paperwork burden associated with planning would be approximately 1,090,000 hours in 2003, 1,278,000 hours in 2004, and 827,000 hours in subsequent years.

Vessel Security

Summary

Note: for definition of acronyms throughout this analysis, refer to the list at the beginning of the report.

Implementing the ISPS Code and NVICs could affect about 10,625 vessels.

The estimated cost of complying with the ISPS Code, parts A and B, and

NVICs is PV \$1.129 billion (2003–2012, 7 percent discount rate). Approximately PV \$257 million of this total is attributable to U.S.-flagged SOLAS vessels. The remaining PV \$871 million is attributable to domestic vessels (non-SOLAS) that are affected. In the first year of compliance, the cost of purchasing equipment, hiring security officers, and preparing paperwork is an estimated \$188 million (non-discounted, \$42 million for the U.S.-flagged SOLAS fleet, \$146 million for the domestic fleet). Following initial implementation, the annual cost of compliance is an estimated \$144 million (non-discounted, \$33 million for the U.S.-flagged SOLAS fleet, \$111 million for the domestic fleet).

For the U.S.-flagged SOLAS fleet, approximately 60 percent of the initial cost is for hiring CSOs and training, 24 percent is for vessel equipment, 7 percent is for assigning VSOs to ships, and 9 percent is associated with paperwork (VSAs, VSPs). Following the first year, approximately 79 percent of the cost is for CSOs and training, 3 percent is for vessel equipment, 6 percent is for drilling, 9 percent is for VSOs, and 3 percent is associated with paperwork. CSOs and training are the primary cost driver for U.S.-flagged SOLAS vessels.

For the domestic fleet, approximately 61 percent of the initial cost is for hiring CSOs and training, 25 percent is for vessel equipment, 8 percent is for assigning VSOs to ships, and 6 percent is associated with paperwork (VSAs, VSPs). Following the first year, approximately 82 percent of the cost is for CSOs and training, 1 percent is for vessel equipment, 6 percent is for drilling, 10 percent is for VSOs, and 1 percent is associated with paperwork. As with SOLAS vessels, CSOs are the primary cost driver for the domestic fleet.

We estimate approximately 140,000 burden hours for paperwork during the first year of compliance (36,000 hours for U.S.-flagged SOLAS, 104,000 hours for the domestic fleet). We estimate approximately 7,000 burden hours annually following full implementation of the ISPS Code and NVICs (1,000 hours for U.S.-flagged SOLAS, 6,000 hours for the domestic fleet).

We assume shipping companies would apply the ISPS Code and NVICs differently based on the types of ships they own or operate and whether they operate internationally or domestically. Because an unacceptable amount of detail would be lost if we developed an "average" ship or an "average" company, this analysis calculates cost per affected vessel as well as cost per

affected company to capture characteristics unique to these entities.

Analysis

Period of Analysis

The period of analysis is 2003–2012 (10 years). Companies must come into compliance with the ISPS Code in 2004, but we assume that companies will

purchase equipment and develop security plans prior to the effective date. We assume, therefore, that initial costs will be incurred in 2003, and annual costs will be incurred each year 2004–2012.

Population Affected

The population of affected vessels is derived from the Coast Guard's MSMS database and DOT's National Ferry Database. The U.S.-flagged SOLAS population affected is presented in Table 1. As shown, most of the U.S.-flagged SOLAS fleet are freight ships, tank ships, small passenger vessels, or OSVs. Approximately 170 companies own/operate these vessels.

TABLE 1.—ESTIMATED U.S.-FLAGGED SOLAS POPULATION^{1, 2, 3, 4}

Vessel	Count	Percent ⁵
Freight ship	241	37.6
Freight barge	2	0.3
Tank ship	114	17.8
Tank barge	14	2.2
Towboat	14	2.2
Fishing	39	6.1
Cruise vessel	2	0.3
Other passenger vessel	109	17.0
MODU	2	0.3
OSV	75	11.7
Oil recovery	1	0.2
Research vessel	8	1.2
Industrial vessel	20	3.1
Total	641	100.0

¹ All vessels engaged on international voyages (no GT threshold). There are 96 vessels < 100 GT; there are 112 < 300 GT.

² There are 89 freight ships, 19 tanks ships, 1 MODU, and 1 research vessel owned by MARAD.

³ There are 15 ITBs. They are included in the tank ship population.

⁴ There is 1 recreational vessel that is not included in these estimates.

⁵ Sum may not add to total due to independent rounding.

The domestic population (non-SOLAS) affected is presented in Table 2. As shown, most of the domestic fleet are tank barges, towboats, or OSVs. Approximately 1,950 companies own/operate these vessels.

TABLE 2.—ESTIMATED DOMESTIC POPULATION

Vessel	Count	Percent ¹
Freight ship	99	1.0
Freight barge	262	2.6
Tank ship	34	0.3
Tank barge	2,891	29.0
Towboat >6 meters ²	4,645	46.5
Passenger, ≤100 GT, not ferry	223	2.2
Passenger, ≤100 GT, ferry, >500 passengers	43	0.4
Passenger, ≤100 GT, ferry, ≤500 passengers	435	4.4
Passenger, >100 GT, cruise	2	0.0
Passenger, >100 GT, not ferry	67	0.7
Passenger, >100 GT, ferry, >500 passengers	49	0.5
Passenger, >100 GT, ferry, ≤500 passengers	92	0.9
MODU	159	1.6
OSV	983	9.9
Total	9,984	100.0

¹ Sum may not add to total due to independent rounding.

² Towboats over 50 GT. This is a good proxy for towboats > 6 meters.

Unit Cost Assumptions

Equipment

Costs of equipment are based on extensive research and analysis of several studies that addressed security needs. We estimate annual O&M cost for equipment is 5 percent of the purchase price. Not all vessels would install each piece of equipment. Unit costs of equipment are presented in Table 3.

TABLE 3.—UNIT COST OF EQUIPMENT

Equipment	Initial	Annual
Hand-held metal detector	\$200	\$10
Hand-held radio	200	10
Lock	300	15
Light	400	20
Camera	475	24
Auto-intrusion alarm	500	25
Ship security system (SOLAS only)	2,000	100
Archway metal detector	5,500	275
Portable vapor detector	8,000	400
X-ray baggage machine	39,000	1,950

Personnel, Training, Drilling, and Planning

Costs of personnel and training are based on extensive research and previous Coast Guard analyses that estimated training and planning costs. Personnel and training costs will be incurred each year of the analysis. Drilling costs will be incurred annually, but not initially. Planning costs will be incurred initially and annually, with more costs incurred initially as companies develop their security plans.

We assume costs will vary based on the types of vessels companies own. Companies differ by size and whether or not they are “towing” companies. For the purpose of this analysis, we assume that a large company owns more than 10 vessels (excluding towboats and barges). A small company owns 10 or fewer vessels (excluding towboats and barges).¹ A “towing” company owns only towboats and barges. A “non-towing” company is any other company (it owns only non-towing vessels or it

owns a combination of towboats and non-towing vessels).

We assume that large companies will have a dedicated CSO. Small companies will have a part-time CSO (we estimate 0.25 of a dedicated person). CSOs and key crew will have some form of training annually as refresher courses and to address potential employee turnover within a company. The ISPS Code also requires all CSOs to participate in an annual security exercise; for the purposes of this analysis, these costs have been accounted for in the “Port Security” section. VSOs will be existing personnel on board vessels that will allocate part of their time toward security activities. Towing vessels will not have VSOs. For VSAs and VSPs, we assume the company will prepare the core documents, and there will be an incremental cost for each vessel included in the assessment or plan. The incremental cost added to each plan will be based on the number and type of vessels. We assume each hour of

planning costs an average of \$100/hour. This is a “loaded” labor rate, which means it includes the costs of benefits and other overhead costs. While some employees cost more than this and some cost less, we believe \$100/hour is a reasonable average cost of the employees that would conduct this work. To calculate costs for VSAs and VSPs, we estimated number of hours that would be required initially (plan development and submission) and annually (plan updates), then multiplied by hourly cost.

For drilling, the time required will depend on the number of crewmembers aboard the vessel. We assume each hour of drilling also costs an average of \$100/hour per crewmember (again, a loaded labor rate that represents an average cost of the labor performing these duties). Drilling for all vessels except towboats and barges will be conducted quarterly. Towboats and associated barges will drill under order of the COTP (approximately every 18 months). Table 4 summarizes personnel costs.

TABLE 4.—UNIT COST OF PERSONNEL
[Loaded labor costs]

Personnel	Large company		Small company	
	Initial	Annual	Initial	Annual
CSO	\$150,000	\$150,000	\$37,500	\$37,500
CSO training	3,500	3,500	2,000	2,000
Training of key crew	5,000	5,000	3,500	3,500
VSO	5,000	5,000	5,000	5,000
VSA, non-towing	8,000	400	4,000	200
VSA, towing	1,600	100	800	100
VSP, non-towing	8,000	400	4,000	200
VSP, towing	1,600	100	800	100

Vessel Costs

The following is a summary of the costs for each type of vessel. Company costs are estimated separately. These costs reflect the current state of the industry and the current level of compliance with security rulemakings already in effect, but not cost incurred in response to the events of September 11, 2001. Since neither the ISPS Code nor the NVICs require specific equipment, we estimated what an “average” vessel within each service type would likely install.

¹ Our use of “large” or “small” to characterize a vessel company does not have the same meaning as

the SBA’s definition. SBA uses NAICS, revenues,

and number of employees to determine company size.

Freight Ships and Barges

Tables 5–8 present the per-vessel cost for U.S.-flagged SOLAS and domestic freight ships and freight barges.

TABLE 5.—COST PER U.S.-FLAGGED SOLAS FREIGHT SHIP

[241 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held metal detector	2	\$200	\$400	2	\$10	\$20
Hand-held radio	5	200	1,000	5	10	50
Lock	10	300	3,000	10	15	150
Light	5	400	2,000	5	20	100
Auto-intrusion alarm	5	500	2,500	5	25	125
Ship security system	1	2,000	2,000	1	100	100
Portable vapor detector	1	8,000	8,000	1	400	400
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	16.00 hrs	100/hr	1,600	0.02 hrs	100/hr	2
VSP (incremental cost)	4.00 hrs	100/hr	400	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 15 crew	1,500/drill	6,000
Total cost per vessel	25,900	11,949

TABLE 6.—COST PER U.S.-FLAGGED SOLAS FREIGHT BARGE

[2 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
VSA (incremental cost)	4.00 hrs	\$100/hr	\$400	0.02 hrs	\$100/hr	\$2
VSP (incremental cost)	0.25 hrs	100/hr	25	0.02 hrs	100/hr	2
Total cost per vessel	425	4

TABLE 7.—COST PER DOMESTIC FREIGHT SHIP

[99 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held metal detector	2	\$200	\$400	2	\$10	\$20
Hand-held radio	5	200	1,000	5	10	50
Lock	10	300	3,000	10	15	150
Light	5	400	2,000	5	20	100
Auto-intrusion alarm	5	500	2,500	5	25	125
Portable vapor detector	1	8,000	8,000	1	400	400
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	8.00 hrs	100/hr	800	0.02 hrs	100/hr	2
VSP (incremental cost)	4.00 hrs	100/hr	400	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 15 crew	1,500/drill	6,000
Total cost per vessel	23,100	11,849

TABLE 8.—COST PER DOMESTIC FREIGHT BARGE

[262 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
VSA (incremental cost)	0.02	\$100	\$2	0.02 hrs	100/hr	\$2
VSP (incremental cost)	0.02 hrs	100/hr	2	0.02 hrs	100/hr	2
Total cost per vessel	4	4

Tank Ships and Barges

Tables 9–12 present the per-vessel cost for U.S.-flagged SOLAS and domestic tank ships and tank barges.

TABLE 9.—COST PER U.S.-FLAGGED SOLAS TANK SHIP
[114 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held metal detector	1	\$200	\$200	1	\$10	\$10
Hand-held radio	5	200	1,000	5	10	50
Lock	10	300	3,000	10	15	150
Light	5	400	2,000	5	20	100
Auto-intrusion alarm	5	500	2,500	5	25	125
Ship security system	1	2,000	2,000	1	100	100
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	16.00 hrs	100/hr	1,600	0.02 hrs	100/hr	2
VSP (incremental cost)	4.00 hrs	100/hr	400	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 15 crew	1,500/drill	6,000
Total cost per vessel	17,700	11,539

TABLE 10.—COST PER U.S.-FLAGGED SOLAS TANK BARGE
[14 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
VSA (incremental cost)	4.00 hrs	\$100/hr	\$400	0.02 hrs	\$100/hr	\$2
VSP (incremental cost)	0.08 hrs	100/hr	8	0.02 hrs	100/hr	2
Total cost per vessel	408	4

TABLE 11.—COST PER DOMESTIC TANK SHIP
[34 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held metal detector	1	\$200	\$200	1	\$10	\$10
Hand-held radio	5	200	1,000	5	10	50
Lock	10	300	3,000	10	15	150
Light	5	400	2,000	5	20	100
Auto-intrusion alarm	5	500	2,500	5	25	125
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	8.00 hrs	100/hr	800	0.02 hrs	100/hr	2
VSP (incremental cost)	4.00 hrs	100/hr	400	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 15 crew	1,500/drill	6,000
Total cost per vessel	14,900	11,439

TABLE 12.—COST PER DOMESTIC TANK BARGE
[2,891 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
VSA (incremental cost)	0.02 hrs	\$100/hr	\$2	0.02 hrs	\$100/hr	\$2
VSP (incremental cost)	0.02 hrs	100/hr	2	0.02 hrs	100/hr	2
Total cost per vessel	4	4

Uninspected Vessels

Tables 13–15 present the per-vessel cost for U.S.-flagged SOLAS towboats and fish processors and domestic towboats.

TABLE 13.—COST PER U.S.-FLAGGED SOLAS TOWBOAT
[14 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held radio	1	\$200	\$200	1	\$10	\$10
Lock	3	300	900	3	15	45
Light	2	400	800	2	20	40
Ship security system	1	2,000	2,000	1	100	100
VSA (incremental cost)	8.00 hrs	100/hr	800	0.02 hrs	100/hr	2
VSP (incremental cost)	2.00 hrs	100/hr	200	0.02 hrs	100/hr	2
Total cost per vessel	4,900	199

TABLE 14.—COST PER U.S.-FLAGGED SOLAS FISH PROCESSOR
[39 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held metal detector	1	\$200	\$200	1	\$10	\$10
Hand-held radio	3	200	600	3	10	30
Lock	10	300	3,000	10	15	150
Light	2	400	800	2	20	40
Auto-intrusion alarm	2	500	1,000	2	25	50
Ship security system	1	2,000	2,000	1	100	100
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	8.00 hrs	100/hr	800	0.02 hrs	100/hr	2
VSP (incremental cost)	2.00 hrs	100/hr	200	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 5 crew ..	500/drill	2,000
Total cost per vessel	13,600	7,384

TABLE 15.—COST PER DOMESTIC TOWBOAT
[4,645 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Lock	3	\$300	\$900	3	\$15	\$45
Light	2	400	800	2	20	40
VSA (incremental cost)	0.02 hrs	100/hr	2	0.02 hrs	100/hr	2
VSP (incremental cost)	0.02 hrs	100/hr	2	0.02 hrs	100/hr	2
Total cost per vessel	1,704	89

U.S.-Flagged SOLAS Passenger Vessels

Tables 16 and 17 present the per-vessel cost for U.S.-flagged SOLAS passenger vessels.

TABLE 16.—COST PER U.S.-FLAGGED SOLAS CRUISE VESSEL
[2 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held radio	10	\$200	\$2,000	10	\$10	\$100
Ship security system	1	2,000	2,000	1	100	100
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	24.00 hrs	100/hr	2,400	0.02 hrs	100/hr	2
VSP (incremental cost)	4.00 hrs	100/hr	400	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 20 crew ..	2,000/drill	8,000
Total cost per vessel	11,800	13,204

TABLE 17.—COST PER OTHER U.S.-FLAGGED SOLAS PASSENGER VESSEL
[109 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held metal detector	2	\$200	\$400	2	\$10	\$20
Hand-held radio	5	200	1,000	5	10	50
Lock	20	300	6,000	20	15	300
Auto-intrusion alarm	5	500	2,500	5	25	125
Ship security system	1	2,000	2,000	1	100	100
Archway metal detector	1	5,500	5,500	1	275	275
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	8.00 hrs	100/hr	800	0.02 hrs	100/hr	2
VSP (incremental cost)	2.00 hrs	100/hr	200	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 10 crew	1,000/drill	4,000
Total cost per vessel	23,400	9,874

Passenger Vessels ≤ 100 GT

Tables 18–20 present the per-vessel cost for domestic passenger vessels.

TABLE 18.—COST PER DOMESTIC PASSENGER VESSEL, NOT FERRY
[223 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held metal detector	1	\$200	\$200	1	\$10	\$10
Hand-held radio	5	200	1,000	5	10	50
Lock	10	300	3,000	10	15	150
Light	5	400	2,000	5	20	100
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	8.00 hrs	100/hr	800	0.02 hrs	100/hr	2
VSP (incremental cost)	4.00 hrs	100/hr	400	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 5 crew	500/drill	2,000
Total cost per vessel	12,400	7,314

TABLE 19.—COST PER DOMESTIC FERRY >500 PASSENGERS
[43 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/ item	Total cost
Hand-held metal detector	2	\$200	\$400	2	\$10	\$20
Hand-held radio	5	200	1,000	5	10	50
Lock	10	300	3,000	10	15	150
Light	5	400	2,000	5	20	100
Auto-intrusion alarm	5	500	2,500	5	25	125
Archway metal detector	2	5,500	11,000	2	275	550
Portable vapor detector	1	8,000	8,000	1	400	400
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	8.00 hrs	100/hr	800	0.02 hrs	100/hr	2
VSP (incremental cost)	4.00 hrs	100/hr	400	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 15 crew	1,500/drill	6,000
Total cost per vessel	34,100	12,399

TABLE 20.—COST PER DOMESTIC FERRY ≤500 PASSENGERS
[435 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held metal detector	2	\$200	\$400	2	\$10	\$20
Hand-held radio	5	200	1,000	5	10	50
Lock	10	300	3,000	10	15	150
Light	5	400	2,000	5	20	100

TABLE 20.—COST PER DOMESTIC FERRY ≤500 PASSENGERS—Continued
[435 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Portable vapor detector	1	8,000	8,000	1	400	400
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	8.00 hrs	100/hr	800	0.02 hrs	100/hr	2
VSP (incremental cost)	4.00 hrs	100/hr	400	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 10 crew	1,000/drill	4,000
Total cost per vessel	20,600	9,724

Passenger Vessels > 100 GT

Tables 21–24 present the per-vessel cost for domestic passenger vessels.

TABLE 21.—COST PER DOMESTIC CRUISE VESSEL
[2 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held radio	10	\$200	\$2,000	10	\$10	\$100
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	16.00 hrs	100/hr	1,600	0.02 hrs	100/hr	2
VSP (incremental cost)	4.00 hrs	100/hr	400	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 20 crew	2,000/drill	8,000
Total cost per vessel	9,000	13,104

TABLE 22.—COST PER DOMESTIC PASSENGER VESSEL, NOT FERRY
[67 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held metal detector	1	\$200	\$200	1	\$10	\$10
Hand-held radio	10	200	2,000	10	10	100
Lock	20	300	6,000	20	15	300
Camera	5	475	2,375	5	24	120
Auto-intrusion alarm	10	500	5,000	10	25	250
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	8.00 hrs	100/hr	800	0.02 hrs	100/hr	2
VSP (incremental cost)	4.00 hrs	100/hr	400	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 10 crew	1,000/drill	4,000
Total cost per vessel	21,775	9,784

TABLE 23.—COST PER DOMESTIC FERRY >500 PASSENGERS
[49 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held metal detector	2	\$200	\$400	2	\$10	\$20
Hand-held radio	10	200	2,000	10	10	100
Lock	20	300	6,000	20	15	300
Camera	5	475	2,375	5	24	120
Auto-intrusion alarm	10	500	5,000	10	25	250
Archway metal detector	2	5,500	11,000	2	275	550
Portable vapor detector	1	8,000	8,000	1	400	400
X-ray baggage machine	1	39,000	39,000	1	1,950	1,950
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	8.00 hrs	100/hr	800	0.02 hrs	100/hr	2
VSP (incremental cost)	4.00 hrs	100/hr	400	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 15 crew	1,500/drill	6,000

TABLE 23.—COST PER DOMESTIC FERRY >500 PASSENGERS—Continued
[49 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Total cost per vessel	79,975	14,694

TABLE 24.—COST PER DOMESTIC FERRY >500 PASSENGERS
[92 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held metal detector	2	\$200	\$400	2	\$10	\$20
Hand-held radio	5	200	1,000	5	10	50
Lock	20	300	6,000	20	15	300
Auto-intrusion alarm	5	500	2,500	5	25	125
Archway metal detector	2	5,500	11,000	2	275	550
Portable vapor detector	1	8,000	8,000	1	400	400
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	8.00 hrs	100/hr	800	0.02 hrs	100/hr	2
VSP (incremental cost)	4.00 hrs	100/hr	400	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 10 crew	1,000/drill	4,000
Total cost per vessel	35,100	10,449

MODUs

Tables 25 and 26 present the per-vessel cost for U.S.-flagged SOLAS and domestic MODUs.

TABLE 25.—COST PER U.S.-FLAGGED SOLAS MODU
[2 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held radio	5	\$200	\$1,000	5	\$10	\$50
Lock	10	300	3,000	10	15	150
Light	5	400	2,000	5	20	100
Auto-intrusion alarm	5	500	2,500	5	25	125
Ship security system	1	2,000	2,000	1	100	100
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	16.00 hrs	100/hr	1,600	0.02 hrs	100/hr	2
VSP (incremental cost)	4.00 hrs	100/hr	400	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 10 crew	1,000/drill	4,000
Total cost per vessel	17,500	9,529

TABLE 26.—COST PER DOMESTIC MODU
[159 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held radio	5	\$200	\$1,000	5	\$10	\$50
Lock	10	300	3,000	10	15	150
Light	5	400	2,000	5	20	100
Auto-intrusion alarm	5	500	2,500	5	25	125
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	16.00 hrs	100/hr	1,600	0.02 hrs	100/hr	2
VSP (incremental cost)	4.00 hrs	100/hr	400	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 10 crew	1,000/drill	4,000
Total cost per vessel	15,500	9,429

OSVs

Tables 27 and 28 present the per-vessel cost for U.S.-flagged SOLAS and domestic OSVs.

TABLE 27.—COST PER U.S.-FLAGGED SOLAS OSV
[75 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held metal detector	1	\$200	\$200	1	\$10	\$10
Hand-held radio	3	200	600	3	10	30
Lock	10	300	3,000	10	15	150
Light	2	400	800	2	20	40
Auto-intrusion alarm	2	500	1,000	2	25	50
Ship security system	1	2,000	2,000	1	100	100
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	8.00 hrs	100/hr	800	0.02 hrs	100/hr	2
VSP (incremental cost)	4.00 hrs	100/hr	400	0.02 hrs	100/hr	2
Quarterly drills	1hr, 4 crew ...	400/drill	1,600
Total cost per vessel	13,800	6,984

TABLE 28.—COST PER DOMESTIC OSV
[983 Vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held metal detector	1	\$200	\$200	1	\$10	\$10
Hand-held radio	3	200	600	3	10	30
Lock	10	300	3,000	10	15	150
Light	2	400	800	2	20	40
Auto-intrusion alarm	2	500	1,000	2	25	50
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	8.00 hrs	100/hr	800	0.02 hrs	100/hr	2
VSP (incremental cost)	4.00 hrs	100/hr	400	0.02 hrs	100/hr	2
Quarterly drills	1hr, 4 crew ...	400/drill	1,600
Total cost per vessel	11,800	6,884

Other U.S.-Flagged SOLAS Vessels

Tables 29–31 present the per-vessel cost for other U.S.-flagged SOLAS vessels.

TABLE 29.—COST PER U.S.-FLAGGED SOLAS OIL RECOVERY VESSEL
[1 Vessel affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held radio	3	\$200	\$600	3	\$10	\$30
Lock	10	300	3,000	10	15	150
Light	2	400	800	2	20	40
Auto-intrusion alarm	2	500	1,000	2	25	50
Ship security system	1	2,000	2,000	1	100	100
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	8.00 hrs	100/hr	800	0.02 hrs	100/hr	2
VSP (incremental cost)	2.00 hrs	100/hr	200	0.02 hrs	100/hr	2
Quarterly drills	1hr, 3 crew ...	300/drill	1,200
Total cost per vessel	13,400	6,574

TABLE 30.—COST PER U.S.-FLAGGED SOLAS RESEARCH VESSEL
[8 vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held radio	3	\$200	\$600	3	\$10	\$30
Lock	10	300	3,000	10	15	150
Light	2	400	800	2	20	40
Auto-intrusion alarm	2	500	1,000	2	25	50
Ship security system	1	2,000	2,000	1	100	100

TABLE 30.—COST PER U.S.-FLAGGED SOLAS RESEARCH VESSEL—Continued
[8 vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	8.00 hrs	100/hr	800	0.02 hrs	100/hr	2
VSP (incremental cost)	2.00 hrs	100/hr	200	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 5 crew ..	500/drill	2,000
Total cost per vessel	13,400	7,374

TABLE 31.—COST PER U.S.-FLAGGED SOLAS INDUSTRIAL VESSEL
[20 vessels affected]

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Hand-held radio	1	\$200	\$200	1	\$10	\$10
Lock	3	300	900	3	15	45
Light	2	400	800	2	20	40
Ship security system	1	2,000	2,000	1	100	100
VSO	1	5,000	5,000	1	5,000	5,000
VSA (incremental cost)	8.00 hrs	100/hr	800	0.02 hrs	100/hr	2
VSP (incremental cost)	2.00 hrs	100/hr	200	0.02 hrs	100/hr	2
Quarterly drills	1 hr, 5 crew ..	500/drill	2,000
Total cost per vessel	9,900	7,199

Company Costs

The cost per company depends on the number and type of vessels a company owns. For this analysis, companies are defined as follows.

- Large non-towing company—company owns more than 10 vessels, none is a towboat or barge; there are 19 companies in our population
 - Large towing company—company owns more than 10 vessels, at least one is a towboat or barge; there are 10 companies in our population
 - Small non-towing company—company owns 10 or fewer vessels, none is a towboat or barge; there are 616 companies in our population
 - Small towing company—company owns only towboats or barges, regardless of the number; there are 1,398 companies in our population
 - U.S.-flagged SOLAS company—treated as a large non-towing company; there are 167 companies in our population
- The cost per company by type is presented in Table 32.

TABLE 32.—COST PER COMPANY BY TYPE

Company type	Initial	Annual
Large non-towing company:		
CSO	\$150,000	\$150,000
CSO training	3,500	3,500
Training of key crew	5,000	5,000
VSA	8,000	400
VSP	8,000	400
Total cost	174,500	159,300
Large towing company:		
CSO	\$150,000	\$150,000
CSO training	3,500	3,500
Training of key crew	5,000	5,000
VSA	1,600	100
VSP	1,600	100
Total cost	161,700	158,700
Small non-towing company:		
CSO	\$37,500	\$37,500
CSO training	2,000	2,000
Training of key crew	3,500	3,500
VSA	4,000	200

TABLE 32.—COST PER COMPANY BY TYPE—Continued

Company type	Initial	Annual
VSP	4,000	200
Total cost	51,000	43,400
Small towing company:		
CSO	\$37,500	\$37,500
CSO training	2,000	2,000
Training of key crew	3,500	3,500
VSA	800	100
VSP	800	100
Total cost	44,600	43,200

To calculate total costs per company, we added the company-level costs (above) and the vessel-level costs (equipment, VSO, incremental VSA and VSP costs, drilling). Example calculations are presented below. The companies in these examples are good representations of the types of companies affected.

Example 1—U.S.-Flagged SOLAS Company

Company A owns 2 freight ships, 4 industrial vessels, 20 OSVs, and 4 research vessels, all of which are U.S.-flagged SOLAS vessels. The initial and annual costs for this company are presented in Table 33.

TABLE 33.—EXAMPLE COST FOR U.S.-FLAGGED SOLAS COMPANY

Cost	Initial			Annual	
	Number	Cost/item	Total cost	Cost/item	Total cost
Company (Table 32)	1	\$174,500	\$174,500	\$159,300	\$159,300
Freight ships (Table 5)	2	25,900	51,800	11,949	23,898
Industrial vessels (Table 31)	4	9,900	39,600	7,199	28,796
OSVs (Table 27)	20	13,800	276,000	6,984	139,680
Research vessels (Table 30)	4	13,400	53,600	7,374	29,496
Total company cost	595,500	381,170

Example 2a—Large Non-Towing Company (No Passenger Vessels)

Company B owns 19 MODUs and 25 OSVs (*i.e.*, no passenger vessels). The initial and annual costs for this company are presented in Table 34.

TABLE 34.—EXAMPLE COST FOR LARGE NON-TOWING COMPANY
[No Passenger Vessels]

Cost	Number	Initial		Annual	
		Cost/item	Total cost	Cost/item	Total cost
Company (Table 32)	1	\$174,500	\$174,500	\$159,300	\$159,300
MODUs (Table 26)	19	15,500	294,500	9,429	179,151
OSVs (Table 28)	25	11,800	295,000	6,884	172,100
Total company cost	764,000	510,551

Example 2b—Large Non-Towing Company (With Passenger Vessels)

Company C owns 9 ferries 100 GT or less carrying fewer than 500 passengers, 11 ferries over 100 GT carrying more than 500 passengers, and 14 ferries over 100 GT carrying fewer than 500 passengers. The initial and annual costs for this company are presented in Table 35.

TABLE 35.—EXAMPLE COST FOR LARGE NON-TOWING COMPANY
[With Passenger Vessels]

Cost	Number	Initial		Annual	
		Cost/item	Total cost	Cost/item	Total cost
Company (Table 32)	1	\$174,500	\$174,500	\$159,300	\$159,300
Ferries, ≤ 100 GT, ≤ 500 pass. (Table 20)	9	20,600	185,400	9,724	87,516
Ferries, > 100 GT, > 500 pass. (Table 23)	11	79,975	879,725	14,694	161,634
Ferries, > 100 GT, ≤ 500 pass. (Table 24)	14	35,100	491,400	10,449	146,286

TABLE 35.—EXAMPLE COST FOR LARGE NON-TOWING COMPANY—Continued
[With Passenger Vessels]

Cost	Number	Initial		Annual	
		Cost/item	Total cost	Cost/item	Total cost
Total company cost	1,731,025	544,736

Example 3—Large Towing Company

Company D owns 12 OSVs and 5 towboats. The initial and annual costs for this company are presented in Table 36.

TABLE 36.—EXAMPLE COST FOR LARGE TOWING COMPANY

Cost	Number	Initial		Annual	
		Cost/item	Total cost	Cost/item	Total cost
Company (Table 32)	1	\$161,700	\$161,700	\$158,700	\$158,700
OSVs (Table 28)	12	11,800	141,600	6,884	82,608
Towboats (Table 15)	5	1,704	8,520	89	445
Total company cost	311,820	241,753

Example 4—Small Non-Towing Company

Company E owns 3 ferries 100 GT or less carrying more than 500 passengers and 6 ferries 100 GT or less carrying fewer than 500 passengers. The initial and annual costs for this company are presented in Table 37.

TABLE 37.—EXAMPLE COST FOR SMALL NON-TOWING COMPANY

Cost	Number	Initial		Annual	
		Cost/item	Total cost	Cost/item	Total cost
Company (Table 32)	1	\$51,000	\$51,000	\$43,400	\$43,400
Large ferries (Table 19)	3	34,100	102,300	12,399	37,197
Small ferries (Table 20)	6	20,600	123,600	9,724	58,344
Total company cost	276,900	138,941

Example 5—Small Towing Company

Company F owns 1 freight barge, 6 tank barges, and 6 towboats. The initial and annual costs for this company are presented in Table 38.

TABLE 38.—EXAMPLE COST FOR SMALL TOWING COMPANY

Cost	Number	Initial		Annual	
		Cost/item	Total cost	Cost/item	Total cost
Company (Table 32)	1	\$44,600	\$44,600	\$43,200	\$43,200
Freight barges (Table 8)	1	4	4	4	4
Tank barges (Table 12)	6	4	24	4	24
Towboats (Table 15)	6	1,704	10,224	89	534
Total company cost	54,852	43,762

Total National Cost of Vessel Security

The national cost of vessel security is the sum of the individual cost estimated for each company affected. National cost is discounted to its PV at 7 percent (2003–2012). The national initial and annual cost is presented in Table 39.

TABLE 39.—TOTAL NATIONAL PV COST FOR VESSEL SECURITY, IN \$MILLIONS
[2003–2012, 7 Percent discount rate]

	U.S.-flagged SOLAS	Domestic	Total	PV total
2003 (initial)	\$42	\$146	\$188	\$188
2004 (annual)	33	111	144	135
2005 (annual)	33	111	144	126
2006 (annual)	33	111	144	118
2007 (annual)	33	111	144	110

TABLE 39.—TOTAL NATIONAL PV COST FOR VESSEL SECURITY, IN \$MILLIONS—Continued
[2003–2012, 7 Percent discount rate]

	U.S.-flagged SOLAS	Domestic	Total	PV total
2008 (annual)	33	111	144	103
2009 (annual)	33	111	144	96
2010 (annual)	33	111	144	90
2011 (annual)	33	111	144	84
2012 (annual)	33	111	144	79
Total cost (\$m)	339	1,145	1,484	1,129

Table 40 presents the national cost for different elements of compliance for U.S.-flagged SOLAS and domestic vessels (these costs are not discounted).

TABLE 40.—TOTAL NATIONAL INITIAL AND ANNUAL COST BY ELEMENT OF COMPLIANCE, IN \$MILLIONS

Cost	Initial				Annual			
	U.S.-flagged SOLAS	Percent of total	Domestic	Percent of total	U.S.-flagged SOLAS	Percent of total	Domestic	Percent
Equipment	\$10	24	\$36	25	\$1	3	\$1	1
Drilling	0	0	0	0	2	6	7	6
VSO	3	7	11	8	3	9	11	10
CSO, training	25	60	89	61	26	79	91	82
Paperwork	4	9	10	6	1	3	1	1
Total	42	100	146	100	33	100	111	100

As shown, CSOs and training are the driving costs both initially and annually. In the initial year, equipment accounts for approximately 25 percent of the total cost. Following implementation, drilling and VSO costs are a notable portion of the costs.

Facility Security

Summary

Note: for definition of acronyms throughout this analysis, refer to the list at the beginning of the report.

Implementing the ISPS Code could affect about 4,400 facilities.

The estimated cost for U.S. facilities to implement the ISPS Code is PV \$4.4 billion (2003 to 2012, 7 percent discount rate). Approximately PV \$2.4 billion of this total is attributable to facilities engaged in the transfer of hazardous bulk liquids (petroleum, edible oils, and liquefied gases). The remaining PV \$2.0 billion is attributable to facilities that receive ships on international voyages or carry more than 149 passengers. During the initial year of compliance, the cost is attributable to purchasing equipment, hiring security officers, and preparing paperwork. The initial cost is an estimated \$963 million (non-discounted, \$478 million for the facilities with hazardous bulk liquids, \$485 million for the other facilities). Following initial implementation, the annual cost is an estimated \$535 million (non-discounted, \$300 million for the

facilities with hazardous bulk liquids, \$235 million for the other facilities).

Approximately 46 percent of the initial cost is for installing or upgrading equipment, 37 percent for hiring and training FSOs², 13 percent for hiring additional security guards, and 4 percent for paperwork (FSAs and FSPs). Following the first year, approximately 4 percent of the annual cost is for O&M for equipment, 66 percent for FSOs, 23 percent for security guards, 7 percent for drills, and approximately 1 percent for paperwork (updating FSAs and FSPs). Installing or upgrading equipment and FSOs are the primary cost drivers for the cost of facility security.

The paperwork burden for developing FSAs and FSPs is approximately 465,000 hours during the initial year. In subsequent years, the annual burden is approximately 17,000 hours.

Analysis

Period of Analysis

The period of analysis is 2003–2012 (10 years). Implementation will become effective in 2004, but we assume that companies will purchase equipment and develop security plans prior to the effective date. We assume, therefore,

² The ISPS Code provides requirements for “Port Facilities.” The Coast Guard, however, differentiates between ports and facilities in domestic regulations. As a result, for the purposes of this cost analysis, the terms PFSSO, PFSA, and PFSP have been replaced with FSO, FSA, and FSP for the facility security section.

that initial costs will be incurred in 2003, and annual costs will be incurred each year 2004–2012.

Population Affected

Implementing the ISPS Code would affect about 4,400 facilities that engage in the transfer of hazardous substances or that service vessels on international voyages. The facility population affected is presented in Table 41. To determine the number of facilities we used data from the U.S. Army Corps of Engineers, DOT’s National Ferry Database, and the Coast Guard’s MSMS database.

TABLE 41.—ESTIMATED FACILITY POPULATION 1 2 3

Facility	Count	Percent ⁴
Container and break-bulk	263	6.0
Dry bulk	255	5.8
Hazardous bulk liquid	2,718	6.2
Hazardous substance (other)	565	12.9
Other bulk liquid	150	3.4
Ferry	306	7.0
Other passenger	108	2.5
Total	4,365	100.0

¹ Facilities that transfer, store, or otherwise contain hazardous cargoes.

² Facilities servicing vessels that carry more than 149 passengers.

³ Facilities receiving ships on international voyages.

⁴ Sum may not add to total due to independent rounding.

Container and break-bulk facilities include container, general cargo, and Ro-Ro facilities. Hazardous bulk liquid facilities include petroleum, liquefied gases, and edible oils. Other hazardous substances are dry hazardous cargoes specified in 33 CFR 126, 127, and 154. The cargoes are further discussed in 49 CFR 172 and 46 CFR 148.

We recognize that not all facilities will incur the same cost for personnel salaries, hire the same number of security guards or spend the same hours in drafting FSAs and FSPs. For the purpose of this analysis we have divided the facility population in two. One group is composed of one third of all facilities and would pay high salaries, hire more guards, and spend more time drafting FSAs and FSPs than the other group composed of two thirds of the total population. Facilities in the first group are addressed in this analysis as "A" and facilities in the second group as "B."

Unit Cost Assumptions

Equipment

Costs of equipment are based on internal Coast Guard data and market research. We estimate annual O&M cost for equipment is 5 percent of the purchase price. Not all facilities will install each piece of equipment. The unit costs for upgrading or installing equipment are presented in Table 42.

TABLE 42.—UNIT COST OF EQUIPMENT

Equipment	Initial	Annual
Hand-held radio	\$200	\$10
Upgrading/installing gates	100,000	5,000
Upgrading/installing CCTV	130,000	6,500
Upgrading/installing lights	200,000	10,000
Upgrading/installing communications system	300,000	15,000
Upgrading/installing fencing	500,000	25,000

Personnel, Training, Drilling, and Planning

Costs of personnel and training are based on extensive research and previous Coast Guard analyses that estimated training and planning costs.

We assume that group A facilities will have a dedicated FSO while facilities in group B will have a part-time FSO (we estimate 0.25 or 0.5 of a dedicated person depending on the type of facility). FSOs or key facility personnel will have training annually as refresher courses and to address potential employee turnover within a facility. We also assume that the cost of a full time FSO is \$150,000 per year. The ISPS Code requires all FSOs to participate in an annual security exercise; for the purposes of this analysis, these costs have been accounted for in the "Port Security" section.

The cost of a security guard was determined using the annual wage

estimate from the 2001 National Occupation Employment and Wage Statistics published by the BLS. We took the annual salary for the upper 90th percentile of \$28,660 per year and multiplied (or "loaded") this estimate by an assumed average benefit multiplier of 1.4 to create a wage that reflects current industry benefits and administrative costs paid by owners and operators. We assumed this higher-than-average wage reflects a full-time, permanent wage for skilled labor.

Personnel and training costs will be incurred each year of the analysis. Drilling costs will be incurred quarterly, but not initially. Planning costs will be incurred initially and annually, with more costs incurred initially as facilities develop their security plans.

We assume each hour of planning or drilling costs an average of \$100/hour. This is a "loaded" labor rate, which means it includes the costs of benefits and other overhead costs. While some employees cost more than this and some cost less, we believe \$100/hour is a reasonable average cost of the employees that would conduct this work. Drilling for all facilities will be conducted following initial implementation of the ISPS Code. We assume that conducting a quarterly drill would take about 2 hours per facility. We also assume that group A facilities will use 20 people in conducting the drill and that group B facilities will use 5 people. Table 43 summarizes personnel costs.

TABLE 43.—UNIT COST OF PERSONNEL

Personnel	Group A		Group B dry bulk		Group B other	
	Initial	Annual	Initial	Annual	Initial	Annual
FSO	\$150,000	\$150,000	\$75,000	\$75,000	\$37,500	\$37,500
Security guard	40,000	40,000	40,000	40,000	40,000	40,000
FSA	8,000	400	4,000	100	4,000	100
FSP	8,000	400	4,000	100	4,000	100
Training	5,000	5,000	3,500	3,500	3,500	3,500
Quarterly drill	4,000	1,000	1,000

Facility costs

Facilities differ greatly from one another, and they must do a variety of activities to implement the ISPS Code. Within group A or group B facilities, we

assume that a facility will have to upgrade/install equipment based on cargo received and current level of compliance with the ISPS Code. For example, to comply with the ISPS Code a facility may upgrade/install CCTV,

lights, or fencing, but it does not have to do all three. For illustration purposes, Tables 44 and 45 present potential costs for a non-specific group A facility and a non-specific group B facility.

TABLE 44.—INITIAL AND ANNUAL COST FOR A NON-SPECIFIC GROUP A FACILITY

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Communications system	1	\$300,000	\$300,000	1	\$15,000	\$15,000
Gates	1	100,000	100,000	1	5,000	5,000
Hand-held radio	18	200	3,600	18	10	180

TABLE 44.—INITIAL AND ANNUAL COST FOR A NON-SPECIFIC GROUP A FACILITY—Continued

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Security guards	9	40,000	360,000	9	40,000	360,000
FSO	1	150,000	150,000	1	150,000	150,000
Training	1	5,000	5,000	1	5,000	5,000
FSA	80 hrs	100/hr	8,000	4 hrs	100/hr	400
FSP	80 hrs	100/hr	8,000	4 hrs	100/hr	400
Quarterly drills	4	4,000	16,000
Base cost per facility	934,600	551,980
Cost per facility with CCTV	1	130,000	\$1,064,600	1	6,500	\$558,480
Cost per facility with lights	1	200,000	1,134,600	1	10,000	561,980
Cost per facility with fencing	1	500,000	1,434,600	1	25,000	576,980

TABLE 45.—INITIAL AND ANNUAL COST FOR A NON-SPECIFIC GROUP B FACILITY

Item	Initial			Annual		
	Number	Cost/item	Total cost	Number	Cost/item	Total cost
Communications system	1	\$300,000	\$300,000	1	\$15,000	\$15,000
Gates	1	100,000	100,000	1	5,000	5,000
Hand-held radio	18	200	3,600	18	10	180
Security guards	3	40,000	120,000	3	40,000	120,000
FSO	1	37,500	37,500	1	37,500	37,500
Training	1	3,500	3,500	1	3,500	3,500
FSA	40 hrs	100/hr	4,000	1 hr	100/hr	100
FSP	40 hrs	100/hr	4,000	1 hr	100/hr	100
Quarterly drills	4	1,000	4,000
Base cost per facility	572,600	185,380
Cost per facility with CCTV	1	130,000	702,600	1	6,500	191,880
Cost per facility with lights	1	200,000	772,600	1	10,000	195,380
Cost per facility with fencing	1	500,000	1,072,600	1	25,000	210,380

The estimated percentage of facilities that would need to purchase, install, or upgrade security measures is presented in Table 46. The figure in each cell represents the percentage of facilities of that type that would install or employ the various security items.

TABLE 46.—ESTIMATED PERCENTAGE OF FACILITIES THAT WILL PURCHASE OR ENHANCE SECURITY MEASURES, BY FACILITY TYPE ^{1, 2, 3}

Item	Container, break-bulk	Dry bulk	Haz. bulk liquid	Haz. sub other	Other bulk liquid	Ferry	Other passenger
Hand-held radio	5	70	5	5	10	5	5
Gates	30	70	10	5	10	60 (A), 80 (B)	5
CCTV	5	10	5	5	10	10	5
Lights	5	60	5	5	10	10	5
Coms system	5	0	5	5	10	0	5
Fencing	5	20	5	5	10	50	5
Security guards	30	70	10	5	10	60 (A), 80 (B)	5

¹ Facilities that transfer, store, or otherwise contain hazardous cargoes.

² Facilities servicing vessels that carry more than 149 passengers.

³ Facilities receiving ships on international voyages.

Tables 47 through 60 present initial and annual costs of complying with the ISPS Code for different types of facilities.

TABLE 47.—INITIAL AND ANNUAL COST FOR CONTAINER OR BREAK-BULK FACILITIES, GROUP A
[87 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Coms system	4 (5%)	1	\$300,000	\$1,200,000	1	\$15,000	\$60,000
Gates	26 (30%)	1	100,000	2,600,000	1	5,000	130,000
Hand-held radio	4 (5%)	18	200	14,400	18	10	720
CCTV	4 (5%)	1	130,000	520,000	1	6,500	26,000

TABLE 47.—INITIAL AND ANNUAL COST FOR CONTAINER OR BREAK-BULK FACILITIES, GROUP A—Continued
[87 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Lights	4 (5%)	1	200,000	800,000	1	10,000	40,000
Fencing	4 (5%)	1	500,000	2,000,000	1	25,000	100,000
Security guards	26 (30%)	15	40,000	15,600,000	15	40,000	15,600,000
FSO	87 (100%)	1	150,000	13,050,000	1	150,000	13,050,000
Training	87 (100%)	1	5,000	435,000	1	5,000	435,000
FSA	87 (100%)	1	8,000	696,000	1	400	34,800
FSP	87 (100%)	1	8,000	696,000	1	400	34,800
Quarterly drills	87 (100%)	1	16,000	1,392,000
Total cost	37,611,400	30,903,320

TABLE 48.—INITIAL AND ANNUAL COST FOR CONTAINER OR BREAK-BULK FACILITIES, GROUP B
[176 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Coms system	9 (5%)	1	\$300,000	\$2,700,000	1	\$15,000	\$135,000
Gates	53 (30%)	1	100,000	5,300,000	1	5,000	265,000
Hand-held radio	9 (5%)	18	200	32,400	18	10	1,620
CCTV	9 (5%)	1	130,000	1,170,000	1	6,500	58,500
Lights	9 (5%)	1	200,000	1,800,000	1	10,000	90,000
Fencing	9 (5%)	1	500,000	4,500,000	1	25,000	225,000
Security guards	53 (30%)	4	40,000	8,480,000	4	40,000	8,480,000
FSO	176 (100%)	1	37,500	6,600,000	1	37,500	6,600,000
Training	176 (100%)	1	3,500	616,000	1	3,500	616,000
FSA	176 (100%)	1	4,000	704,000	1	100	17,600
FSP	176 (100%)	1	4,000	704,000	1	100	17,600
Quarterly drills	176 (100%)	1	4,000	704,000
Total cost	32,606,400	17,210,320

TABLE 49.—INITIAL AND ANNUAL COST FOR DRY BULK FACILITIES, GROUP A
[84 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Gates	59 (70%)	1	\$100,000	\$5,900,000	1	\$5,000	\$295,000
Hand-held radio	59 (70%)	2	200	23,600	2	10	1,180
CCTV	8 (10%)	1	130,000	1,040,000	1	6,500	52,000
Lights	50 (60%)	1	200,000	10,000,000	1	10,000	500,000
Fencing	17 (20%)	1	500,000	8,500,000	1	25,000	425,000
Security guards	59 (70%)	2	40,000	4,720,000	2	40,000	4,720,000
FSO	84 (100%)	1	150,000	12,600,000	1	150,000	12,600,000
Training	84 (100%)	1	5,000	420,000	1	5,000	420,000
FSA	84 (100%)	1	8,000	672,000	1	400	33,600
FSP	84 (100%)	1	8,000	672,000	1	400	33,600
Quarterly drills	84 (100%)	1	16,000	1,344,000
Total cost	44,547,600	20,424,380

TABLE 50.—INITIAL AND ANNUAL COST FOR DRY BULK FACILITIES, GROUP B
[171 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Gates	120 (70%)	1	\$100,000	\$12,000,000	1	\$5,000	\$600,000
Hand-held radio	120 (70%)	2	200	48,000	2	10	2,400
CCTV	17 (10%)	1	130,000	2,210,000	1	6,500	110,500
Lights	103 (60%)	1	200,000	20,600,000	1	10,000	1,030,000
Fencing	34 (20%)	1	500,000	17,000,000	1	25,000	850,000

TABLE 50.—INITIAL AND ANNUAL COST FOR DRY BULK FACILITIES, GROUP B—Continued
[171 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Security guards	120 (70%)	1	40,000	4,800,000	1	40,000	4,800,000
FSO	171 (100%)	1	75,000	12,825,000	1	75,000	12,825,000
Training	171 (100%)	1	3,500	598,500	1	3,500	598,500
FSA	171 (100%)	1	4,000	684,000	1	100	17,100
FSP	171 (100%)	1	4,000	684,000	1	100	17,100
Quarterly drills	171 (100%)	1	4,000	684,000
Total cost	71,449,500	21,534,600

TABLE 51.—INITIAL AND ANNUAL COST FOR HAZARDOUS BULK LIQUID FACILITIES, GROUP A
[897 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Coms system	45 (5%)	1	\$300,000	\$13,500,000	1	\$15,000	\$675,000
Gates	90 (10%)	1	100,000	9,000,000	1	5,000	450,000
Hand-held radio	45 (5%)	18	200	162,000	18	10	8,100
CCTV	45 (5%)	1	130,000	5,850,000	1	6,500	292,500
Lights	45 (5%)	1	200,000	9,000,000	1	10,000	450,000
Fencing	45 (5%)	1	500,000	22,500,000	1	25,000	1,125,000
Security guards	90 (10%)	9	40,000	32,400,000	9	40,000	32,400,000
FSO	897 (100%)	1	150,000	134,550,000	1	150,000	134,550,000
Training	897 (100%)	1	5,000	4,485,000	1	5,000	4,485,000
FSA	897 (100%)	1	8,000	7,176,000	1	400	358,800
FSP	897 (100%)	1	8,000	7,176,000	1	400	358,800
Quarterly drills	897 (100%)	1	16,000	14,352,000
Total cost	245,799,000	189,505,200

TABLE 52.—INITIAL AND ANNUAL COST FOR HAZARDOUS BULK LIQUID FACILITIES, GROUP B
[1,821 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Coms system	91 (5%)	1	\$300,000	\$27,300,000	1	\$15,000	\$1,365,000
Gates	182 (10%)	1	100,000	18,200,000	1	5,000	910,000
Hand-held radio	91 (5%)	18	200	327,600	18	10	16,380
CCTV	91 (5%)	1	130,000	11,830,000	1	6,500	591,500
Lights	91 (5%)	1	200,000	18,200,000	1	10,000	910,000
Fencing	91 (5%)	1	500,000	45,500,000	1	25,000	2,275,000
Security guards	182 (10%)	3	40,000	21,840,000	3	40,000	21,840,000
FSO	1,821 (100%)	1	37,500	68,287,500	1	37,500	68,287,500
Training	1,821 (100%)	1	3,500	6,373,500	1	3,500	6,373,500
FSA	1,821 (100%)	1	4,000	7,284,000	1	100	182,100
FSP	1,821 (100%)	1	4,000	7,284,000	1	100	182,100
Quarterly drills	1,821 (100%)	1	4,000	7,284,000
Total cost	232,426,600	110,217,080

TABLE 53.—INITIAL AND ANNUAL COST FOR HAZARDOUS SUBSTANCE (OTHER) FACILITIES, GROUP A
[186 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Coms system	9 (5%)	1	\$300,000	\$2,700,000	1	\$15,000	\$135,000
Gates	9 (5%)	1	100,000	900,000	1	5,000	45,000
Hand-held radio	9 (5%)	18	200	32,400	18	10	1,620
CCTV	9 (5%)	1	130,000	1,170,000	1	6,500	58,500
Lights	9 (5%)	1	200,000	1,800,000	1	10,000	90,000
Fencing	9 (5%)	1	500,000	4,500,000	1	25,000	225,000

TABLE 53.—INITIAL AND ANNUAL COST FOR HAZARDOUS SUBSTANCE (OTHER) FACILITIES, GROUP A—Continued
[186 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Security guards	9 (5%)	9	40,000	3,240,000	9	40,000	3,240,000
FSO	186 (100%)	1	150,000	27,900,000	1	150,000	27,900,000
Training	186 (100%)	1	5,000	930,000	1	5,000	930,000
FSA	186 (100%)	1	8,000	1,488,000	1	400	74,400
FSP	186 (100%)	1	8,000	1,488,000	1	400	74,400
Quarterly drills	186 (100%)	1	16,000	2,976,000
Total cost	46,148,400	35,749,920

TABLE 54.—INITIAL AND ANNUAL COST FOR HAZARDOUS SUBSTANCE (OTHER) FACILITIES, GROUP B
[379 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Coms system	19 (5%)	1	\$300,000	\$5,700,000	1	\$15,000	\$285,000
Gates	19 (5%)	1	100,000	1,900,000	1	5,000	95,000
Hand-held radio	19 (5%)	18	200	68,400	18	10	3,420
CCTV	19 (5%)	1	130,000	2,470,000	1	6,500	123,500
Lights	19 (5%)	1	200,000	3,800,000	1	10,000	190,000
Fencing	19 (5%)	1	500,000	9,500,000	1	25,000	475,000
Security guards	19 (5%)	3	40,000	2,280,000	3	40,000	2,280,000
FSO	379 (100%)	1	37,500	14,212,500	1	37,500	14,212,500
Training	379 (100%)	1	3,500	1,326,500	1	3,500	1,326,500
FSA	379 (100%)	1	4,000	1,516,000	1	100	37,900
FSP	379 (100%)	1	4,000	1,516,000	1	100	37,900
Quarterly drills	379 (100%)	1	4,000	1,516,000
Total cost	44,289,400	20,582,720

TABLE 55.—INITIAL AND ANNUAL COST FOR OTHER BULK LIQUID FACILITIES, GROUP A (50 FACILITIES)

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Coms system	5 (10%)	1	\$300,000	\$1,500,000	1	\$15,000	\$75,000
Gates	5 (10%)	1	100,000	500,000	1	5,000	25,000
Hand-held radio	5 (10%)	18	200	18,000	18	10	900
CCTV	5 (10%)	1	130,000	650,000	1	6,500	32,500
Lights	5 (10%)	1	200,000	1,000,000	1	10,000	50,000
Fencing	5 (10%)	1	500,000	2,500,000	1	25,000	125,000
Security guards	5 (10%)	2	40,000	400,000	2	40,000	400,000
FSO	50 (100%)	1	150,000	7,500,000	1	150,000	7,500,000
Training	50 (100%)	1	5,000	250,000	1	5,000	250,000
FSA	50 (100%)	1	8,000	400,000	1	400	20,000
FSP	50 (100%)	1	8,000	400,000	1	400	20,000
Quarterly drills	50 (100%)	1	16,000	800,000
Total cost	15,118,000	9,298,400

TABLE 56.—INITIAL AND ANNUAL COST FOR OTHER BULK LIQUID FACILITIES, GROUP B
[100 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Coms system	10 (10%)	1	\$300,000	\$3,000,000	1	\$15,000	\$150,000
Gates	10 (10%)	1	100,000	1,000,000	1	5,000	50,000
Hand-held radio	10 (10%)	18	200	36,000	18	10	1,800
CCTV	10 (10%)	1	130,000	1,300,000	1	6,500	65,000
Lights	10 (10%)	1	200,000	2,000,000	1	10,000	100,000
Fencing	10 (10%)	1	500,000	5,000,000	1	25,000	250,000
Security guards	10 (10%)	1	40,000	400,000	1	40,000	400,000

TABLE 56.—INITIAL AND ANNUAL COST FOR OTHER BULK LIQUID FACILITIES, GROUP B—Continued
[100 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
FSO	100 (100%)	1	75,000	7,500,000	1	75,000	7,500,000
Training	100 (100%)	1	3,500	350,000	1	3,500	350,000
FSA	100 (100%)	1	4,000	400,000	1	100	10,000
FSP	100 (100%)	1	4,000	400,000	1	100	10,000
Quarterly drills	100 (100%)	1	4,000	400,000
Total cost	21,386,000	9,286,800

TABLE 57.—INITIAL AND ANNUAL COST FOR FERRY TERMINALS, GROUP A
[101 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Gates	61 (60%)	1	\$100,000	\$6,100,000	1	\$5,000	\$305,000
Hand-held radio	5 (5%)	12	200	12,000	12	10	600
CCTV	10 (10%)	1	130,000	1,300,000	1	6,500	65,000
Lights	10 (10%)	1	200,000	2,000,000	1	10,000	100,000
Fencing	51 (50%)	1	500,000	25,500,000	1	25,000	1,275,000
Security guards	61 (60%)	6	40,000	14,640,000	6	40,000	14,640,000
FSO	101 (100%)	1	150,000	15,150,000	1	150,000	15,150,000
Training	101 (100%)	1	5,000	505,000	1	5,000	505,000
FSA	101 (100%)	1	8,000	808,000	1	400	40,400
FSP	101 (100%)	1	8,000	808,000	1	400	40,400
Quarterly drills	101 (100%)	1	16,000	1,616,000
Total cost	66,823,000	33,737,400

TABLE 58.—INITIAL AND ANNUAL COST FOR FERRY TERMINALS, GROUP B
[205 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Gates	164 (80%)	1	\$30,000	4,920,000	1	\$1,500	\$246,000
Hand-held radio	10 (5%)	12	200	24,000	12	10	1,200
CCTV	21 (10%)	1	130,000	2,730,000	1	6,500	136,500
Lights	21 (10%)	1	200,000	4,200,000	1	10,000	210,000
Fencing	103 (50%)	1	500,000	51,500,000	1	25,000	2,575,000
Security guards	164 (80%)	2	40,000	13,120,000	2	40,000	13,120,000
FSO	205 (100%)	1	37,500	7,687,500	1	37,500	7,687,500
Training	205 (100%)	1	3,500	717,500	1	3,500	717,500
FSA	205 (100%)	1	4,000	820,000	1	100	20,500
FSP	205 (100%)	1	4,000	820,000	1	100	20,500
Quarterly drills	205 (100%)	1	4,000	820,000
Total cost	86,539,000	25,554,700

TABLE 59.—INITIAL AND ANNUAL COST FOR PASSENGER TERMINALS, GROUP A
[36 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Coms system	2 (5%)	1	\$300,000	\$600,000	1	\$15,000	\$30,000
Gates	2 (5%)	1	100,000	200,000	1	5,000	10,000
Hand-held radio	2 (5%)	18	200	7,200	18	10	360
CCTV	2 (5%)	1	130,000	260,000	1	6,500	13,000
Lights	2 (5%)	1	200,000	400,000	1	10,000	20,000
Fencing	2 (5%)	1	500,000	1,000,000	1	25,000	50,000
Security guards	2 (5%)	15	40,000	1,200,000	15	40,000	1,200,000
FSO	36 (100%)	1	150,000	5,400,000	1	150,000	5,400,000
Training	36 (100%)	1	5,000	180,000	1	5,000	180,000

TABLE 59.—INITIAL AND ANNUAL COST FOR PASSENGER TERMINALS, GROUP A—Continued
[36 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
FSA	36 (100%)	1	8,000	288,000	1	400	14,400
FSP	36 (100%)	1	8,000	288,000	1	400	14,400
Quarterly drills	36 (100%)	1	16,000	576,000
Total cost	9,823,200	7,508,160

TABLE 60.—INITIAL AND ANNUAL COST FOR PASSENGER TERMINALS, GROUP B
[72 Facilities]

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Coms system	4 (5%)	1	\$300,000	\$1,200,000	1	\$15,000	\$60,000
Gates	4 (5%)	1	100,000	400,000	1	5,000	20,000
Hand-held radio	4 (5%)	18	200	14,400	18	10	720
CCTV	4 (5%)	1	130,000	520,000	1	6,500	26,000
Lights	4 (5%)	1	200,000	800,000	1	10,000	40,000
Fencing	4 (5%)	1	500,000	2,000,000	1	25,000	100,000
Security guards	4 (5%)	4	40,000	640,000	4	40,000	640,000
FSO	72 (100%)	1	37,500	2,700,000	1	37,500	2,700,000
Training	72 (100%)	1	3,500	252,000	1	3,500	252,000
FSA	72 (100%)	1	4,000	288,000	1	100	7,200
FSP	72 (100%)	1	4,000	288,000	1	100	7,200
Quarterly drills	72 (100%)	1	4,000	288,000
Total cost	9,102,400	4,141,120

Example cost calculations for different facility owners are presented below. The companies in these examples are good representations of the types of companies affected.

Example 1—Ferry Terminal Owner

Company A owns 11 group A and 21 group B terminals. The estimated costs for this company are presented in Table 61.

TABLE 61.—EXAMPLE COST FOR FERRY TERMINAL OWNER

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Group A terminals:							
Gates	7 (60%)	1	\$100,000	\$700,000	1	\$5,000	\$35,000
Hand-held radio	1 (5%)	12	200	2,400	12	10	120
CCTV	1 (10%)	1	130,000	130,000	1	6,500	6,500
Lights	1 (10%)	1	200,000	200,000	1	10,000	10,000
Fencing	6 (10%)	1	500,000	3,000,000	1	25,000	50,000
Security guards	7 (60%)	6	40,000	1,680,000	2	40,000	1,680,000
FSO	11 (100%)	1	150,000	1,650,000	1	150,000	1,650,000
Training	11 (100%)	1	5,000	55,000	1	5,000	55,000
FSA	11 (100%)	1	8,000	88,000	1	400	4,400
FSP	11 (100%)	1	8,000	88,000	1	400	4,400
Quarterly drills	11 (100%)	1	16,000	176,000
Subtotal	7,593,400	3,771,420
Group B terminals:							
Gates	17 (80%)	1	30,000	510,000	1	15,000	25,500
Hand-held radio	1 (5%)	12	200	2,400	12	10	120
CCTV	2 (10%)	1	130,000	260,000	1	6,500	13,000
Lights	2 (10%)	1	200,000	400,000	1	10,000	20,000
Fencing	11 (50%)	1	500,000	5,500,000	1	25,000	275,000
Security guards	17 (80%)	2	40,000	1,360,000	2	40,000	1,360,000
FSO	21 (100%)	1	37,500	787,500	1	37,500	787,500
Training	21 (100%)	1	3,500	73,500	1	3,500	73,500
FSA	21 (100%)	1	4,000	84,000	1	100	2,100
FSP	21 (100%)	1	4,000	84,000	1	100	2,100
Quarterly drills	21 (100%)	1	4,000	84,000

TABLE 61.—EXAMPLE COST FOR FERRY TERMINAL OWNER—Continued

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Subtotal	9,061,400	2,642,820
Grand total	16,654,800	6,414,240

Example 2—Dry Bulk Facility Owner

Company B owns 7 group A and 13 group B dry bulk facilities. The estimated costs for this company are presented in Table 62.

TABLE 62.—EXAMPLE COST FOR DRY BULK FACILITY OWNER

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Group A facilities:							
Gates	5 (70%)	1	\$100,000	\$500,000	1	\$5,000	\$25,000
Hand-held radio	5 (70%)	2	200	2,000	2	10	100
CCTV	1 (10%)	1	130,000	130,000	1	6,500	6,500
Lights	4 (60%)	1	200,000	800,000	1	10,000	40,000
Fencing	1 (20%)	1	500,000	500,000	1	25,000	25,000
Security guards	5 (70%)	2	40,000	400,000	2	40,000	400,000
FSO	7 (100%)	1	150,000	1,050,000	1	150,000	1,050,000
Training	7 (100%)	1	5,000	35,000	1	5,000	35,000
FSA	7 (100%)	1	8,000	56,000	1	400	2,800
FSP	7 (100%)	1	8,000	56,000	1	400	2,800
Quarterly drills	7 (100%)	1	16,000	112,000
Subtotal	3,529,000	1,699,200
Group B facilities:							
Gates	9 (70%)	1	\$100,000	\$900,000	1	\$1,500	\$45,000
Hand-held radio	9 (70%)	2	200	3,600	2	10	180
CCTV	1 (10%)	1	130,000	130,000	1	6,500	6,500
Lights	8 (60%)	1	200,000	1,600,000	1	10,000	80,000
Fencing	3 (20%)	1	500,000	1,500,000	1	25,000	75,000
Security guards	9 (70%)	1	40,000	360,000	1	40,000	360,000
FSO	13 (100%)	1	75,000	975,000	1	75,000	975,000
Training	13 (100%)	1	3,500	45,500	1	3,500	45,500
FSA	13 (100%)	1	4,000	52,000	1	100	1,300
FSP	13 (100%)	1	4,000	52,000	1	100	1,300
Quarterly drills	13 (100%)	1	4,000	52,000
Subtotal	5,618,100	1,641,780
Grand total	9,147,100	3,340,980

Example 3—Petroleum Facility Owner

Company C owns 7 group A and 13 group B petroleum facilities. The estimated costs for this company are presented in Table 63.

TABLE 63.—EXAMPLE COST FOR PETROLEUM FACILITY OWNER

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Group A facilities:							
Gates	1 (10%)	1	\$100,000	\$100,000	1	\$5,000	\$5,000
Security guards	1 (10%)	9	40,000	360,000	9	40,000	360,000
FSO	7 (100%)	1	150,000	1,050,000	1	150,000	1,050,000
Training	7 (100%)	1	5,000	35,000	1	5,000	35,000
FSA	7 (100%)	1	8,000	56,000	1	400	2,800
FSP	7 (100%)	1	8,000	56,000	1	400	2,800

TABLE 63.—EXAMPLE COST FOR PETROLEUM FACILITY OWNER—Continued

Item	Number (%) estimated to purchase/draft	Initial			Annual		
		Number	Cost/item	Total cost	Number	Cost/item	Total cost
Quarterly drills	7 (100%)	1	16,000	112,000
Subtotal	1,657,000	1,567,600
Group B facilities:							
Coms system	1 (5%)	1	\$300,000	\$300,000	1	\$15,000	\$15,000
Gates	1 (10%)	1	100,000	100,000	1	5,000	5,000
Hand-held radio	1 (5%)	18	200	3,600	18	10	180
CCTV	1 (5%)	1	130,000	130,000	1	6,500	6,500
Lights	1 (5%)	1	200,000	200,000	1	10,000	10,000
Fencing	1 (5%)	1	500,000	500,000	1	25,000	25,000
Security guards	1 (10%)	3	40,000	120,000	3	40,000	120,000
FSO	13 (100%)	1	37,500	487,500	1	37,500	487,500
Training	13 (100%)	1	3,500	45,500	1	3,500	45,500
FSA	13 (100%)	1	4,000	52,000	1	100	1,300
FSP	13 (100%)	1	4,000	52,000	1	100	1,300
Quarterly drills	13 (100%)	1	4,000	52,000
Subtotal	1,990,600	769,280
Grand total	3,647,600	2,336,880

Total national cost for facility security

The national cost of the facility security aspects of the ISPS Code is the sum of the individual costs estimated for each facility affected. National cost is discounted to its PV at 7 percent (2003-2012). The total national initial and annual cost is presented in Table 64.

TABLE 64.—TOTAL NATIONAL PV COST FOR FACILITY SECURITY, IN \$MILLIONS
[2003–2012, 7 Percent Discount Rate]

Year	Con- tainer, break- bulk	Dry bulk	Haz. bulk liquid	Haz. sub other	Other bulk liquid	Ferry	Other pas- senger	Total	PV Total
2003 (initial)	\$70	\$116	\$478	\$90	\$37	\$153	\$19	\$963	\$963
2004 (annual)	48	42	300	55	19	59	12	535	500
2005 (annual)	48	42	300	55	19	59	12	535	467
2006 (annual)	48	42	300	55	19	59	12	535	437
2007 (annual)	48	42	300	55	19	59	12	535	408
2008 (annual)	48	42	300	55	19	59	12	535	381
2009 (annual)	48	42	300	55	19	59	12	535	356
2010 (annual)	48	42	300	55	19	59	12	535	333
2011 (annual)	48	42	300	55	19	59	12	535	311
2012 (annual)	48	42	300	55	19	59	12	535	291
Total	502	494	3,178	585	208	684	127	5,778	4,447

Table 65 presents the national cost for different elements of implementing the ISPS Code for facilities (these costs are not discounted).

TABLE 65.—TOTAL NATIONAL INITIAL AND ANNUAL COST BY ELEMENT OF COMPLIANCE, IN \$MILLIONS

Element	Initial cost	Percent of total	Annual cost	Percent of total
FSA	\$23	2	\$1	0
FSP	23	2	1	0
FSO	335	35	335	63
Training	17	2	17	3
Drilling	0	0	35	7
Security guards	124	13	124	23
Equipment	441	46	22	4
Total	963	100	509	100

As shown, upgrading/installing equipment is the driving costs of implementing the ISPS Code initially. Annually, FSOs are the driving cost. In the initial year, FSOs account for approximately 35 percent of the initial cost and increase in significance to 66 percent annually.

Port Security

Summary

Note: for definition of acronyms throughout this analysis, refer to the list at the beginning of the report.

Implementing the ISPS Code and NVICs could affect stakeholders in 47 COTP AORs containing 361 ports.³ The following analysis details preliminary costs to public and private stakeholders and does not include costs to the Coast Guard.

The preliminary cost estimate of implementing ISPS Code as it pertains to port security is PV \$477 million (2003–2012, 7 percent discount rate). The initial cost of the startup period (June 2003–December 2003) for establishing PSCs and creating PSPs in all AORs is estimated to be \$120 million (non-discounted). Following the startup period, the first year of implementation (2004), consisting of monthly PSC meetings and PSP drill exercises for all AORs, is estimated to be \$106 million (non-discounted). After the first year of implementation, the annual cost of quarterly PSC meetings and PSP drills for all AORs is estimated to be \$46 million (non-discounted). The startup period cost associated with creating PSCs and PSPs for each AOR is the primary cost driver of implementing the ISPS Code at U.S. ports. Both the startup and implementation year period (2003–2004) combined is nearly half of the total 10-year PV cost estimate, making initial development, planning, and testing the primary costs of port security.

Implementing the ISPS Code and complying with NVICs would require all COTPs to develop security committees, plans, and training drills for their AORs, with the participation of maritime transportation stakeholders in their AORs. The above costs to stakeholders would be paperwork, travel, and communication costs associated with participation in PSP implementation.

We estimate 1,090,400 hours of paperwork and other associated planning activities during 2003, the initial period of port security meetings and development. In 2004, the first year of implementation, we estimate the value will rise slightly to 1,278,400 hours of paperwork and other related information and communication activities related to monthly PSC meetings. In subsequent years, we estimate the hours will fall to 827,200 hours annually associated with PSC meetings, PSP revisions, and information drills.

Analysis

Period of Analysis

The period of analysis is from mid 2003 (the startup year) to 2012 (approximately 10 years). The port security aspects would be effective in 2004, so we assume the last 6 months in 2003 of the project to be a startup period of establishing PSCs and creating PSPs for all COTP AORs. We assume, therefore, that initial costs will be incurred in 2003, and annual costs will be incurred each year 2004–2012.

Population Affected

Implementing the ISPS Code would affect stakeholders nationally in 47 COTP AORs containing 361 total ports. The Army Corps of Engineers Navigation Data Center and MARAD provided the data for total ports affected. For this analysis, “ports” include all areas located within or adjacent to a marine environment through which maritime commerce is conducted or people are transported. Consistent with NVIC 9–02, Guidelines for Port Security Committees and Port Security Plans Required for U.S. Ports, and parts A and B of the ISPS Code, PSPs will be developed by PSCs headed by COTPs. COTPs also determine the size and composition of the PSCs. The affected population per COTP AOR is assumed to be stakeholders who participate in the PSC, planning, and drilling. A stakeholder is considered to be any business, organization, (non-Federal) government entity, or individual involved with maritime commerce in a given port area.

We believe the composition and number of stakeholders will vary greatly from AOR to AOR and will be determined by the commercial scope of the ports in each AOR. For the purpose of estimating average costs, we assumed the average level of meeting, planning, and drilling participation to be 200 stakeholders per AOR, based on discussions with COTPs and estimates of average U.S. facility and vessel

presence per port. We understand that some AORs may have higher participation levels and other AORs have very lower participation levels; however, we believe this to be a reasonable national estimate of stakeholder participation per AOR.

Unit Cost Assumptions

The port security implementation cost per stakeholder is expected to be small in comparison to facility and vessel security implementation. Stakeholders are not required to purchase or upgrade materials or services, as in the implementation of the ISPS Code for facilities or vessels. Some companies and facilities are required to have CSOs and FSOs (as detailed in the vessel and facility security sections) attend at least one of the quarterly PSC meetings a year; however, we expect few stakeholders to fully participate in all of the implementation or annual activities for a given COTP AOR. Finally, most stakeholders in large to medium-sized ports have already completed or adopted appropriate and transferable PSPs before the ISPS Code will become effective.

All costs for ISPS Code implementation for port security are related to personnel. Stakeholder hourly costs are assumed to be \$100 per burden hour for managerial personnel and \$35 per burden hour for administrative/clerical personnel. These costs are “loaded” wage rates, which means they include benefits, local travel, and other overhead costs. These rates are based on BLS data and previous Coast Guard analyses that estimated meeting and planning costs. While some employees cost more than this and some cost less, we believe these estimates for the two labor types are reasonable average costs of the employees that would conduct this work.

The stakeholder costs are divided into three hourly activities: PSC meetings, PSP development, and drilling, which include tabletop management drills and administrative drills. PSC meetings are estimated to consume an average of 6 hours for office preparation and meeting time, plus 2 hours of travel time. PSC meetings are monthly for the first 18 months and quarterly thereafter. Initial PSP development and planning is estimated to be a maximum of 80 hours (2 weeks) of non-PSC meeting time in 2003. PSP administrative and management drills are information and communication exercises that will take place at the stakeholder site. Administrative drills will occur twice a year for 2 hours to update company and facility contact information. Management drills will occur four times

³ The ISPS Code provides requirements for “Port Facilities.” The Coast Guard, however, differentiates between ports and facilities in domestic regulations. As a result, for the purposes of this cost analysis, the terms PFSC and PFSP have been replaced with PSC and PSP for the port security section.

a year for 4 hours to exercise PSP information and communication readiness. These activities collectively involve meetings, planning coordination, and communication drills that are information-gathering events.

Costs to stakeholders, therefore, are determined by the labor rates and the number of hours each type of labor will be involved in each activity.

The frequency of the PSC meeting activity, estimated hours, and unit cost

per stakeholder at a full participation level is presented in Table 66, and the frequency of the PSP planning and drill activities, estimated hours, and unit cost per stakeholder at a full participation level is presented in Table 67.

TABLE 66.—PSC MEETING FREQUENCY, HOURS, AND UNIT COST PER STAKEHOLDER

Stakeholder meeting	Hours per meeting	Frequency ¹	Cost per hour	Initial		Annual	
				Total hours per stakeholder	Total cost per stakeholder	Total hours per stakeholder	Total cost per stakeholder
Startup PSC meetings—2003.	8	1/month	\$100	48	\$4,800
Annual PSC meetings:							
2004	8	1/month	100	96	9,600
2005–2012	8	4/year	100	28	2,800

¹ Startup meetings (July–December 2003) consist of monthly planning meetings; the first year of implementation beginning 2004 consists of 12 monthly meetings; meetings for future years will be quarterly.

TABLE 67.—PSP PLANNING AND DRILL FREQUENCY, HOURS, AND UNIT COST PER STAKEHOLDER

Stakeholder activity	Hours per activity	Frequency	Cost per hour	Initial		Annual	
				Total hours per stakeholder	Total cost per stakeholder	Total hours per stakeholder	Total cost per stakeholder
PSP Planning—Year 2003.	80	1/year	\$100	80	\$8,000
PSP Drilling (2004–2012):							
Management	4	4/year	100	16	400
Administrative	2	2/year	35	4	140

Total National Cost for Port Security

We estimated national cost (both initial and annual) to public and private stakeholders for implementation of the ISPS Code for port security. Each cost is discounted to its PV at 7 percent for years 2003–2012. National cost for port security is presented in Table 68.

TABLE 68.—TOTAL NATIONAL PV COST FOR PORT SECURITY, IN \$MILLIONS

[2003–2012, 7 percent discount rate]

	PSPs	Meetings	Drills	Total	PV total
2003 (initial)	\$75	\$45	\$	\$120	\$120
2004 (annual)	90	16	106	99
2005 (annual)	30	16	46	40
2006 (annual)	30	16	46	38
2007 (annual)	30	16	46	35
2008 (annual)	30	16	46	33
2009 (annual)	30	16	46	31
2010 (annual)	30	16	46	29
2011 (annual)	30	16	46	27
2012 (annual)	30	16	46	25
Total cost (\$m)	75	375	144	594	\$477

As shown, the initial cost associated with creating a PSP and holding development PSC meetings for each AOR is the primary cost driver for implementing the ISPS Code at U.S. ports. In addition, both the startup and implementation year periods (2003–2004) combined are nearly half of the total 10-year PV cost, making initial development and planning the primary costs to port security. These estimates are conservative because most COTP AORs have already done some security planning and organization. Furthermore, the level of stakeholder participation may not be as high as 200 per COTP AOR, and stakeholders will not be required to participate in all of the port security activities and drills in a given year.